OpenRG Administrator Manual

Version 5.3

Visit us on the Web at **www.jungo.com**

OpenRG
Administrator Manual

Version 5.3

Jungo Software Technologies Ltd.

OpenRG
Administrator Manual: Version 5.3

This document is available for download at: *http://www.jungo.com/openrg/documentation.html, version 5.3*

Revision: 539-20100516-135736

Table of Contents

Part I Managing Your Gateway

Table of Contents

1

Accessing the Management Console

This chapter describes how to use OpenRG's management console, referred to as the **Web-based Management (WBM)**, which allows you to configure and control all of OpenRG's features and system parameters, using a user-friendly graphical interface. This user-friendly approach is also implemented in the WBM's documentation structure, which is based directly on the WBM's structure. You will find it easy to correspondingly navigate through both the WBM and its documentation.

> Note: Access to the WBM is restricted to wired clients and Web-authenticated or secured wireless clients. In addition, some of the documented WBM features may appear slightly different or may not be available on certain platforms.

To access the Web-based management:

1. Launch a Web browser on a computer in the LAN.

2. In the address bar, type the gateway's name or IP address. The default name is 'http://openrg.home' and the default IP address is 192.168.1.1. The WBM's homepage appears.

1.1 WBM Modes

By default, OpenRG's WBM is displayed in read-only basic mode, providing you with the ability to view your features and system parameters. This mode prevents accessing and changing the gateway's settings, misconfiguration of which may harm its performance.

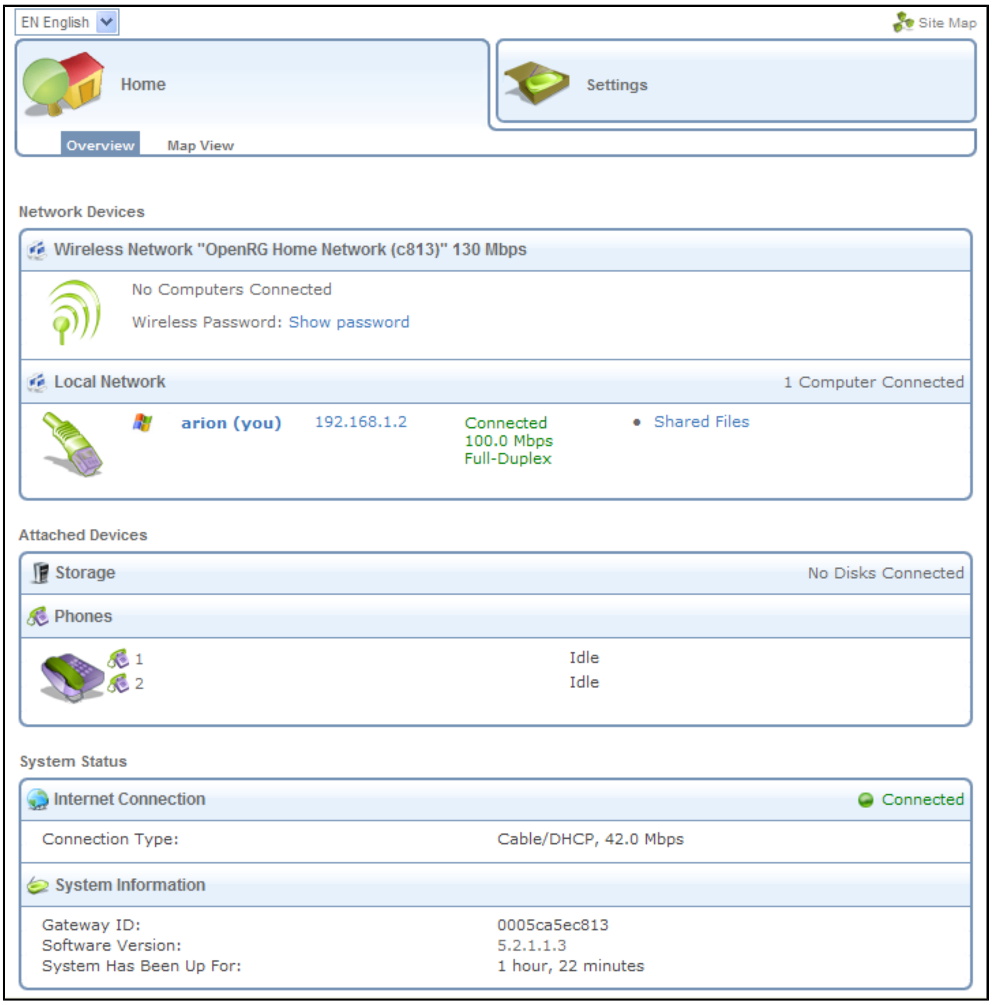


Figure 1.1 WBM – Read Only Basic Mode

To perform configuration actions on your gateway, click the 'Settings' tab. You are required to log in.

Figure 1.2 Settings Login

Enter your username and password, and click 'Continue'. The default username is 'admin' and the default password is 'admin'.

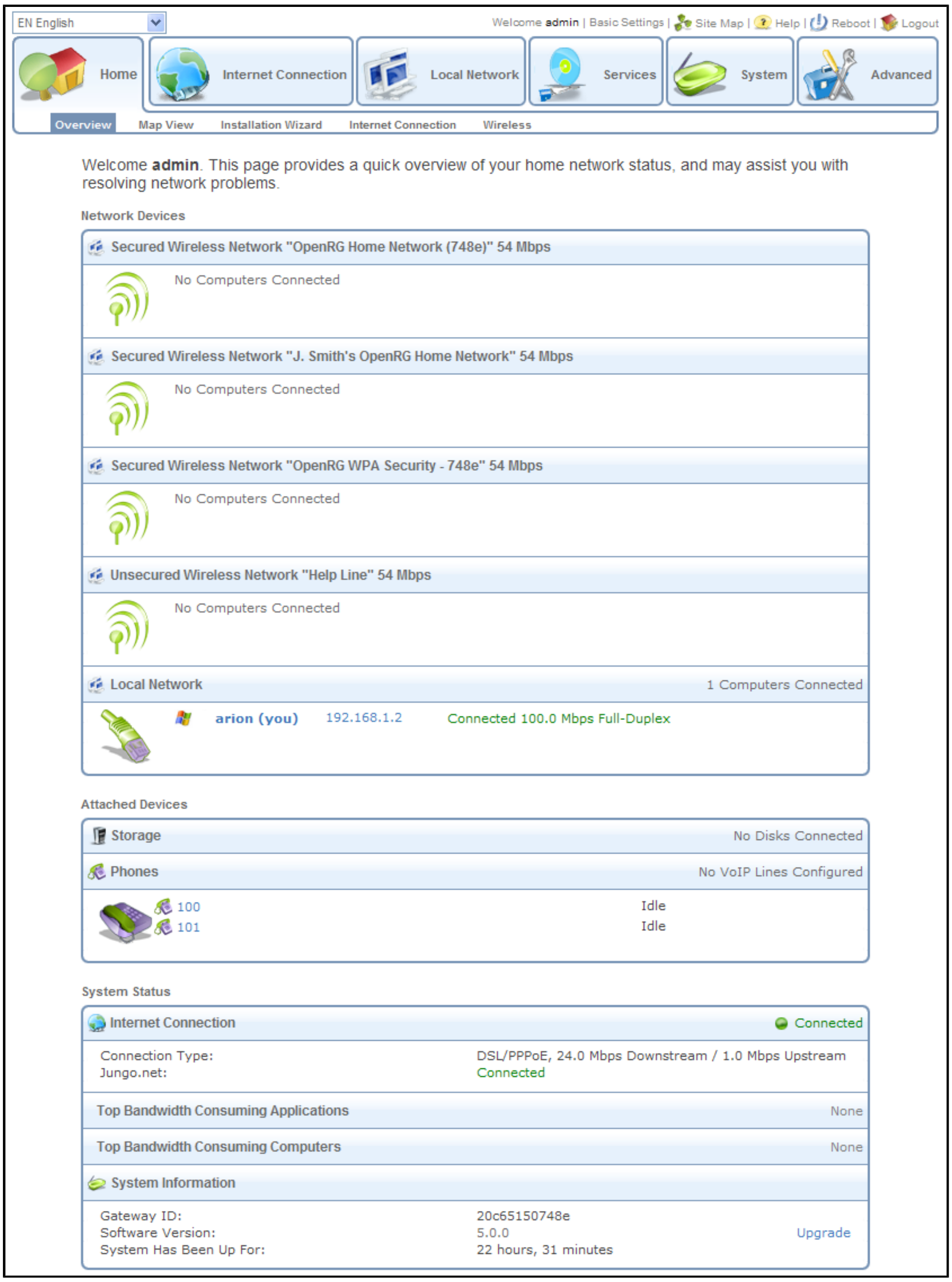


Figure 1.3 WBM – Configuration Mode

By logging in, you have switched from read-only mode to configuration mode. You can now perform various configurations of your gateway, as described in the following sections. To return to read-only mode, click the 'Logout' link located on the top bar.

> Note: Prior to changing default settings of any OpenRG feature, it is recommended that you carefully read the relevant instructions provided in this manual.

A login session will automatically time-out after an extended period of inactivity. If you try to operate the WBM after the session has expired, the 'Login' screen will appear. This feature helps to prevent unauthorized users from accessing your session and changing the gateway's settings.

1.2 Navigational Aids

The Web-based management is a user-friendly interface, designed as a Web site that can be explored with any Web browser. This section illustrates the WBM's page structure and describes its navigational components and their hierarchial manner.

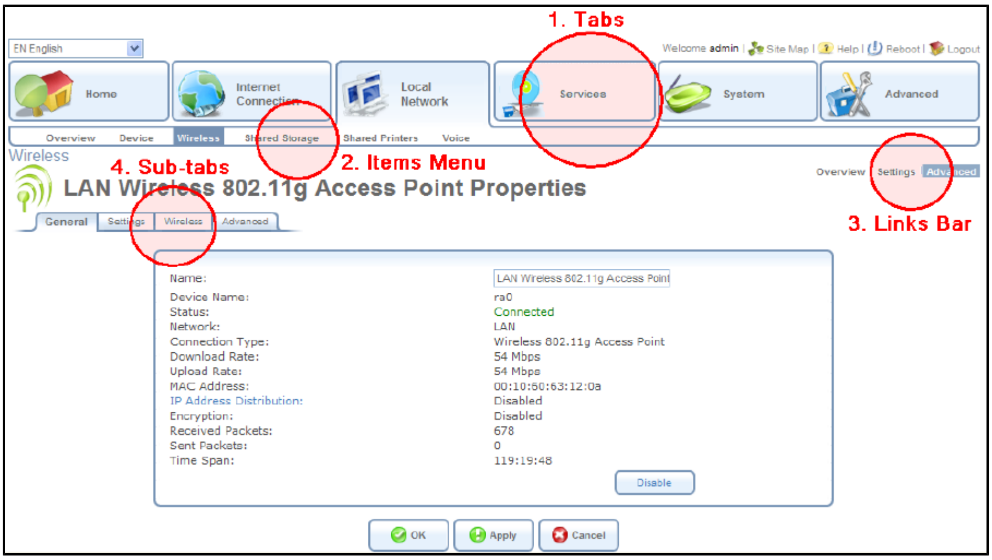


Figure 1.4 Navigation Components

1. The top level navigational aids are the ***Tabs***, grouping the WBM screens into several main subject areas.

   > Note: The following navigational components are only present in the advanced mode of the WBM.

2. A tab may have a ***Menu Items*** bar, listing the different items relevant for the tab.

3. A menu item may have a ***Links Bar***, located at the top-right of the screen. These links further divide the menu item into different subjects.

4. Lastly, a page content, usually a feature's properties page, may have a set of ***Sub-tabs***, providing a division of settings in the form of yet another set of tabs.

> Note: For convenience purposes, the entire WBM part of this User Manual has been constructed in accordance with the structure of the WBM—the chapter structure is identical to the tab structure, sections are written after item menus, etc.

In addition, a constant links bar appears at the top of every WBM page, providing shortcuts to information and control actions.

Figure 1.5 Constant Link Bar

The links bar includes:

- **Site Map –** Leads to a screen representing the hierarchial structure of the WBM.
- **Help** – Leads to your gateway's User Manual.
- **Reboot –** Clicking this link initiates a gateway reboot.
- **Logout** – This link can be used to return to read-only basic mode.

1.3 Tables in the WBM

Tables are structures used throughout the Web-based management. They handle user-defined entries relating to elements such as network connections, local servers, restrictions and configurable parameters. The principles outlined in this section apply to all tables in the WBM.

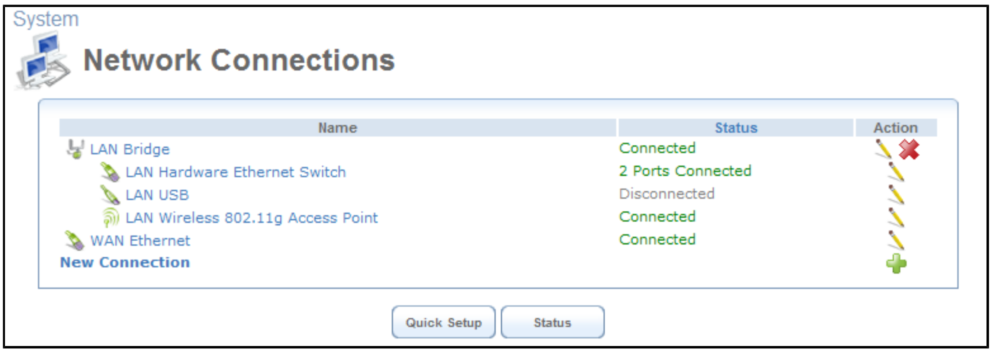


Figure 1.6 Typical Table Structure

Figure 1.6 illustrates a typical table. Each row defines an entry in the table. The following buttons, located in the 'Action' column, enable performing various actions on the table entries.

 Use the **Add** action icon to add a row to the table.

 Use the **Edit** action icon to edit a row in the table.

 Use the **Remove** action icon to remove a row from the table.

 Use the **Download** action icon to download a file from the table.

 Use the **Copy** action icon to copy an item to the clipboard.

 Use the **Move Up** action icon to move a row one step up in the table.

 Use the **Move Down** action icon to move a row one step down in the table.

2

Home

2.1 Overviewing Your Gateway

The 'Overview' screen presents the status of OpenRG's various modules in one convenient location. You can quickly and efficiently view important system details such as the status of your Internet connection, wireless and local networks, as well as hardware peripherals.

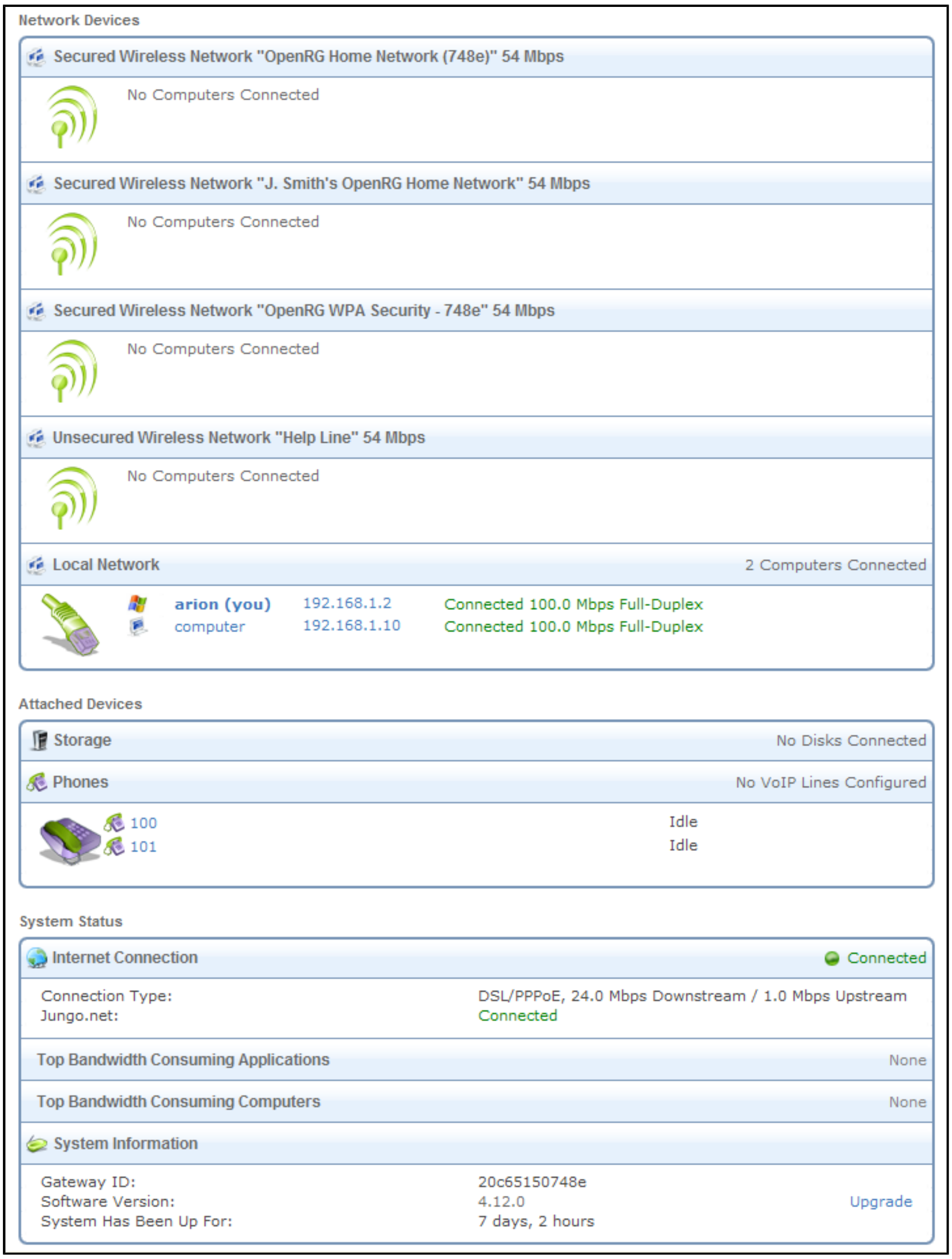


Figure 2.1 Home – Overview

2.1.1 Viewing and Connecting to Your Broadcasted Wireless Network

The 'Network Devices' section displays OpenRG's broadcasted wireless network. To connect to this network from a wireless Windows computer, perform the following:

1. In the Windows system tray, click the wireless connection icon.

Figure 2.2 Wireless Icon in the System Tray

The 'Wireless Network Connection' screen appears, displaying all available wireless networks (also known as Wi-Fi hotspots) in your vicinity. If your gateway is connected and active, you should see its wireless network displayed in this screen. The default wireless network name (SSID) is "OpenRG Home Network (XXXX)", where XXXX are the last four characters of the gateway's **CM MAC** address (as printed on the sticker located at the bottom of the gateway).

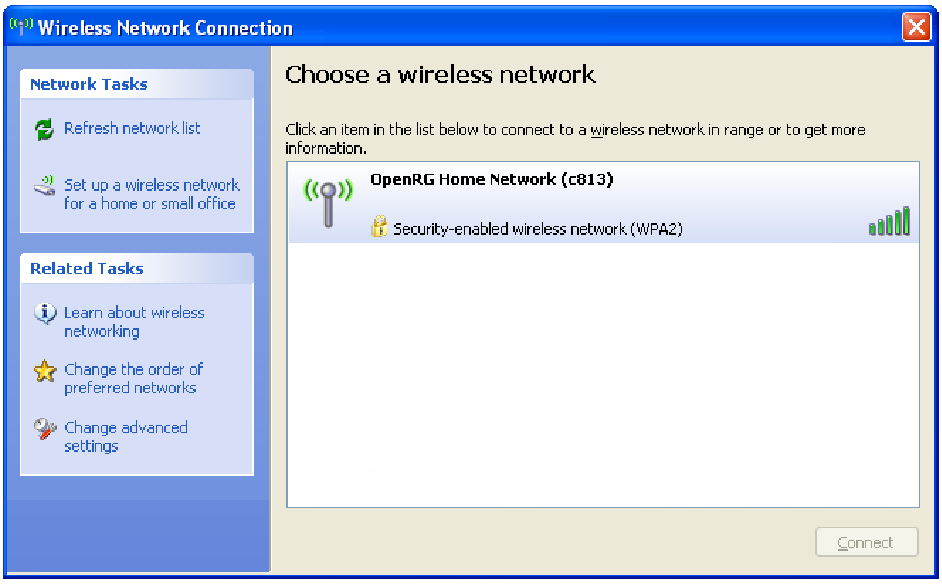


Figure 2.3 Available Wireless Connections

If you do not see your network, refresh the list of detected networks using the 'Refresh network list' link.

2. Select the connection and click the 'Connect' button at the bottom of the screen. The following window appears, requiring you to provide the WPA password (network key).

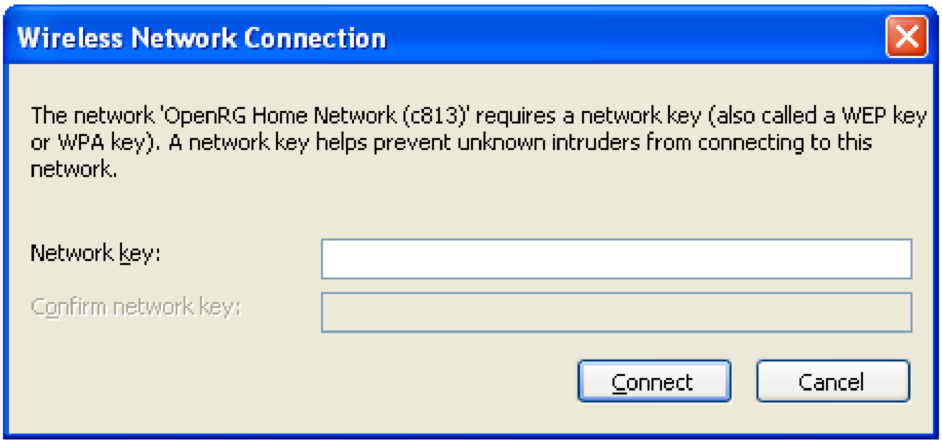


Figure 2.4 WPA Network Key Authentication

Enter the WPA password. This case sensitive password can be found on the sticker located at the bottom of the gateway, and can be changed in the 'Wireless' menu item under the 'Home' tab. After the connection is established, its status changes to 'Connected'.

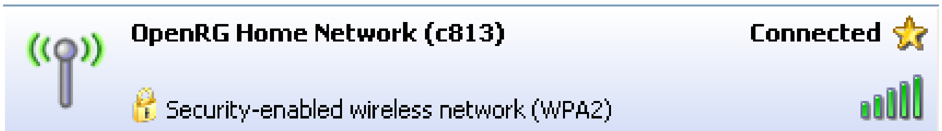


Figure 2.5 Connected Wireless Network

A balloon appears in the notification area, announcing the successful initiation of the wireless connection.

Figure 2.6 Wireless Connection Information

3. If you had selected the default "Medium" security level during the installation wizard, any attempt to browse the Internet will require Web authentication. The following screen appears, requiring you to provide your username and password.

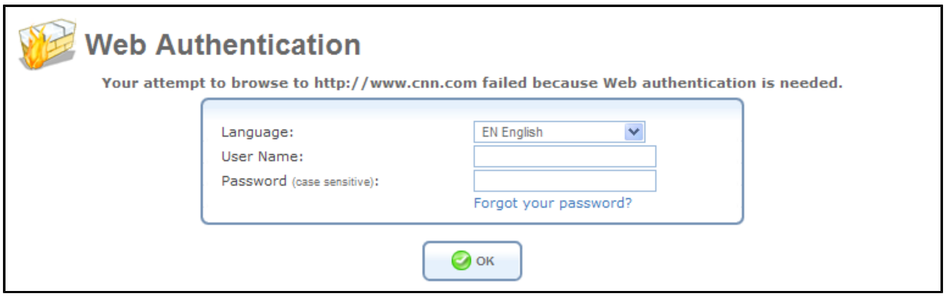


Figure 2.7 Web Authentication

Enter your username and password. You will be redirected to your requested Internet address.

In case you have forgotten your wireless password, click 'Forgot your password?' to display a screen that offers a number of password recovery methods. For more information, refer to Section 6.4.6.3.

4. Open an Internet browser and browse to any site.

The 'Home' screen will now display the connected wireless computer.

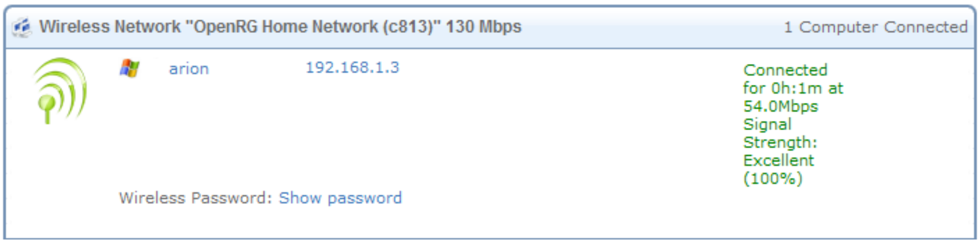


Figure 2.8 Connected Wireless Computer

2.1.2 Authenticating Wireless Network Devices

When attempting to connect to the gateway's network from a wireless computer, a login session is used for authentication and connection. However, you may wish connect other wireless devices to the gateway, such as gaming devices, cameras, etc., in which a login session in is not possible due to the lack of an interface. In such a case, a simple authentication procedure is required in the 'Home' screen.

A preliminary step is to search for the gateway's wireless network from the device itself. Refer to the device's documentation to learn how to perform this search. When OpenRG detects a wireless request, the device is displayed under the relevant wireless connection.

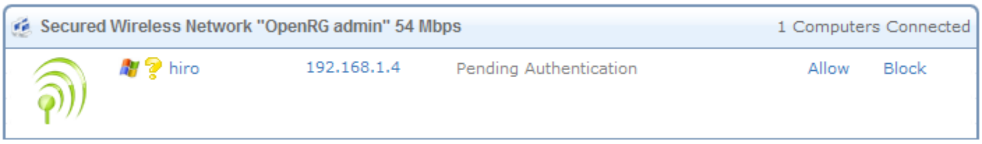


Figure 2.9 Wireless Authentication – Pending

To allow this device to connect to your gateway, click 'Allow'. The screen refreshes, updating the status of the device.

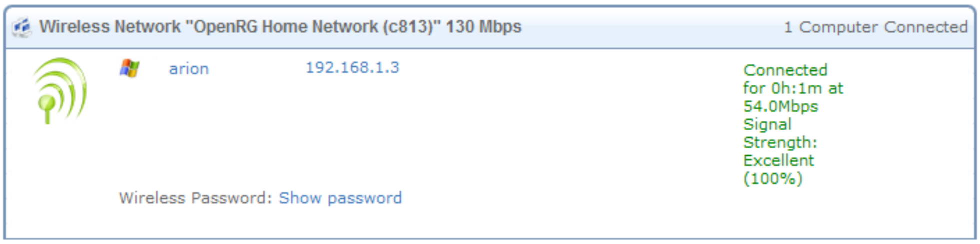


Figure 2.10 Wireless Authentication – Authenticated

The device is now connected. Similarly, you can use the 'Block' link in order to log the device out of your network.

2.1.3 Viewing the Local Network

The 'Network Devices' section also displays OpenRG's local network, which includes all computers that have joined the gateway's network, their IP addresses, and connection speed (see Figure 2.1).

To view more information on a specific computer, click its respective link. The 'Host Information' screen appears.

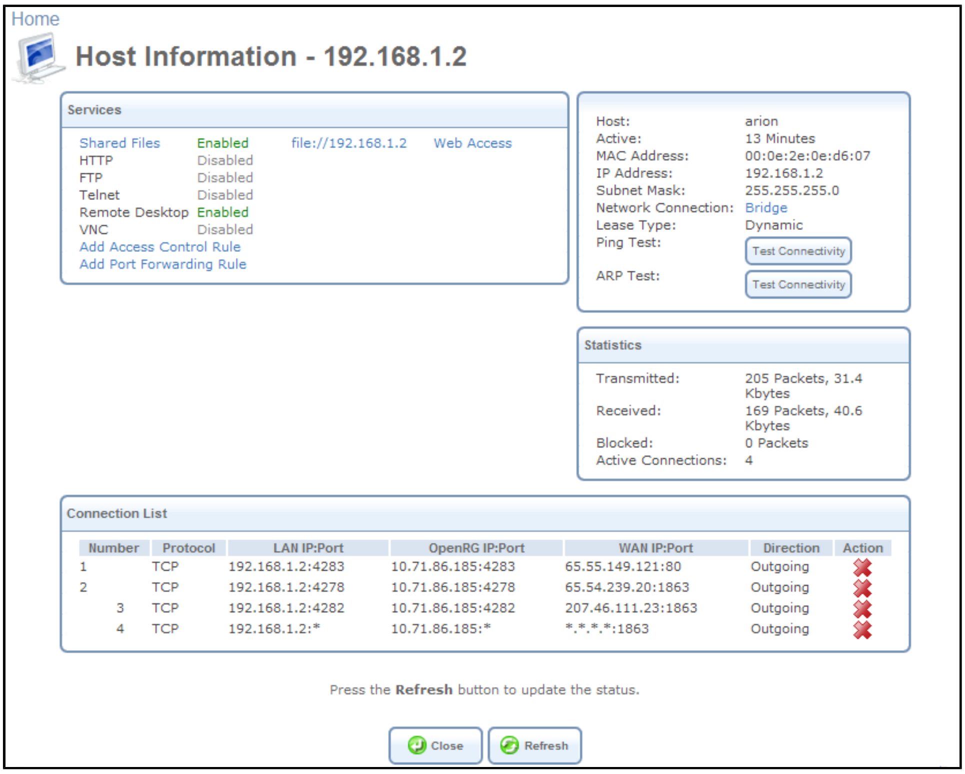


Figure 2.11 Host Information

This screen presents all of the information relevant to the connected computer, such as connection information, available services, and traffic statistics.

Services This section lists the services on the computer that are available to other computers from the LAN. When a service is accessible from the LAN, you can activate it by clicking its name. When a service is accessible via Web access, you can activate it by clicking the 'Web Access' link that appears.

Connection Information This section displays various details regarding the computer's connection settings. In addition, you can run a Ping or ARP test by clicking the respective 'Test Connectivity' button. The tests are performed in the 'Diagnostics' screen (refer to Section 6.8.7).

Statistics This section displays the computer's traffic statistics, such as the number and size of transmitted and received packets.

Connection List This section displays the list of connections opened by the computer on OpenRG's firewall. The table displays the computer's source LAN IP address and port, the gateway's IP address and port to which it is translated, and the destination WAN IP address and port.

2.1.4 Viewing Attached Devices

The 'Attached Devices' section displays the peripheral devices connected to your gateway. These may include storage devices and telephones. For example, connect a storage device and refresh the screen.

Figure 2.12 Connected Storage Device

> Note: The 'Phones' section displays the phone extensions even when there are no connected telephones.

To view more details on the connected printer, click its name link. Note that clicking the larger printer icon redirects you to the 'Print Server' screen, which also contains the list of connected printers.

Similarly, this section displays other devices connected to the gateway. For more information on each device type, refer to its respective section of this manual.

2.1.5 Viewing the System Status

The 'System Status' section of the 'Overview' screen (see Figure 2.1) displays the following details:

- The Internet connection's type, speed capability, and data transmission mode. Click the 'Internet Connection' link for more details.

- The top five bandwidth consuming applications and computers are displayed in their respective sections in descending order. The current downstream and upstream volumes are also displayed for every application and computer. The following links are available:

  - **Top Bandwidth Consuming Applications** This link routes to the 'Internet Connection Utilization' screen under 'QoS', and provides 'By Application' view (for more information, refer to Section 5.3.2.1).
    The bandwidth-consuming applications are grouped into their respective categories, the names of which are displayed in this section. For example, the 'Web' category may include the Web server, the Web access via HTTP/HTTP proxy, and other Internet services. For a full list of the application categories refer to Section 5.3.2.1.
    If you would like to view more details about a specific category and its members, click the 'Top Bandwidth Consuming Applications' link.
    This section may also display user-defined or unknown applications that had not been identified by OpenRG as belonging to one of the pre-defined categories. In this case, their names will appear as links, which you can click to view their details.

  - **Top Bandwidth Consuming Computers** This link routes to the 'Internet Connection Utilization' screen under 'QoS', and provides 'By Computer' view (for

more information, refer to Section 5.3.2.2). If you would like to view more details about a specific bandwidth-consuming computer, click its respective link.

- **Change priorities or limit bandwidth** This link routes to the 'QoS' module's 'General' screen, which enables you to set the WAN devices' Rx/Tx bandwidth,

  and define the QoS profile. For more information, refer to Section 5.3.2.1. For your convenience, this link appears in both of the abovementioned sections.

- Internet connection information, which includes the connection type. Click the 'Internet Connection' headline for more details.

- System information, which includes the gateway's ID, software version and uptime. Click the 'System Information' headline for more details.

2.2 Viewing Your Network with Map View

The 'Map View' screen displays a graphical network map.

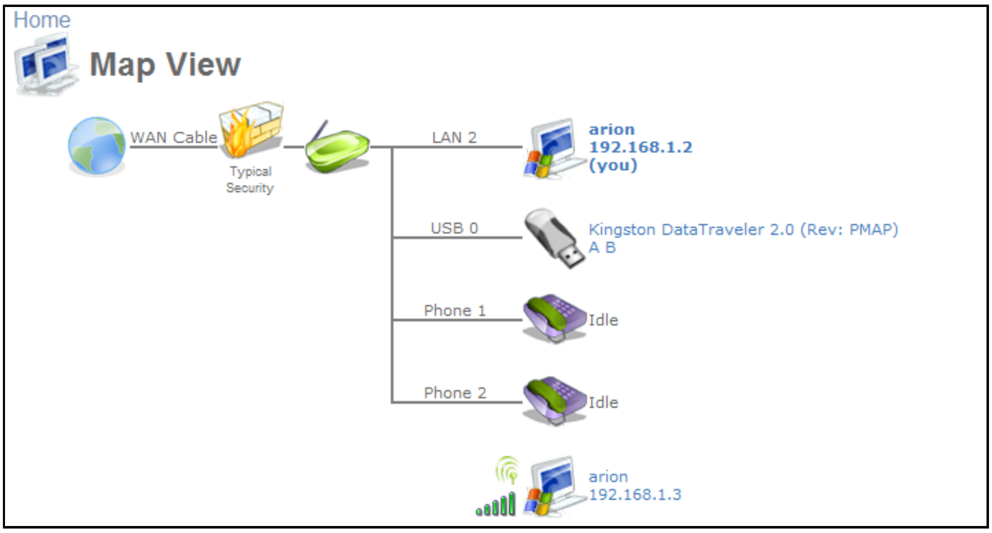


Figure 2.13 Home – Map View

The network map depicts the various network elements, such as the Internet connection, firewall, gateway, and local network computers and peripherals.

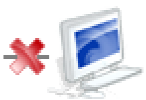
Represents the Internet

Represents the gateway's Firewall. Click this icon to configure your security settings. For more information, refer to Section 5.2.

 Represents your gateway

The network map dynamically represents the network objects connected to your gateway. OpenRG recognizes commercial operating systems and game devices, which are represented by their respective icons.

 Represents a wired/wireless computer (host) connected to the gateway. This host is either a DHCP client that has received an IP lease from OpenRG, or a host with a static IP address, auto-detected by OpenRG. Note that OpenRG will recognize a physically connected host and display it in the Network Map only after network activity from that host has been detected (e.g. trying to browse to the WBM or to surf the Internet). OpenRG will also display incoming connections of types PPTP, L2TP, and IPSec. Click this icon to view network information for the corresponding host.

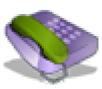
 Represents a host whose DHCP lease has expired and not renewed. The DHCP lease is renewed automatically, unless the host is no longer physically connected to OpenRG. The disconnected host's icon will disappear from the network map during the next scheduled IP lease query, performed by OpenRG's DHCP server.

> Note: This icon also represents a static IP host that has no network activity.

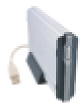
 Represents a Windows™ host connected to your gateway.

 Represents a wireless host connected to your gateway.

 Represents a printer connected to your gateway.

 Represents a telephone connected to your gateway.

 Represents a USB stick (disk-on-key) connected to your gateway.



Represents a USB hard drive connected to your gateway.

OpenRG's standard network map displays devices that the gateway recognized and granted a DHCP lease.

2.3 Installation Wizard

The installation wizard is the first and foremost configuration procedure, which automatically diagnoses your network environment and configures its components. It is a step-by-step procedure that guides you through establishing an Internet connection, a wireless network, and helps you to subscribe for different services by creating a Jungo.net account. The wizard progress box, located at the right hand side of the screen, provides a monitoring tool for its steps during the installation progress.

Figure 2.14 Welcome to OpenRG Installation Wizard

To start the installation wizard, perform the following:

1. Select the desired language and click 'Next' to continue. The 'Login Setup' screen appears.

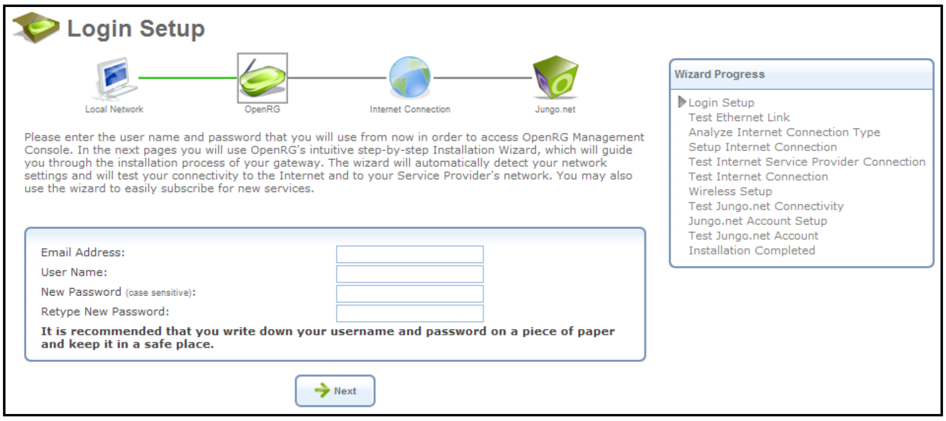


Figure 2.15 Login Setup

2. Enter a valid email address. It will be used by your service provider for sending you important service information.

3. The 'User Name' field is auto-completed by the username part of your email address. You can enter another username, which may only consist of letters and numbers.

4. Enter a password, and retype it in the next field to verify its correctness.

> Note: It is recommended to write down your login details on a piece of paper, and store it in a safe place.

5. Click 'Next'. The wizard is now ready to begin your gateway's configuration.

Figure 2.16 Installation Wizard

6. Click 'Next'. The wizard procedure will commence, performing the steps listed in the progress box consecutively, stopping only if a step fails or if input is required. The following sections describe the wizard steps along with their success/failure scenarios. If a step fails, use the 'Retry' or 'Skip' buttons to continue.

> **Warning:** The installation wizard overrides all Internet connection settings, which you may have previously defined.

2.3.1 Step 1: Test Ethernet Link

The first step is a test of the Ethernet connection.

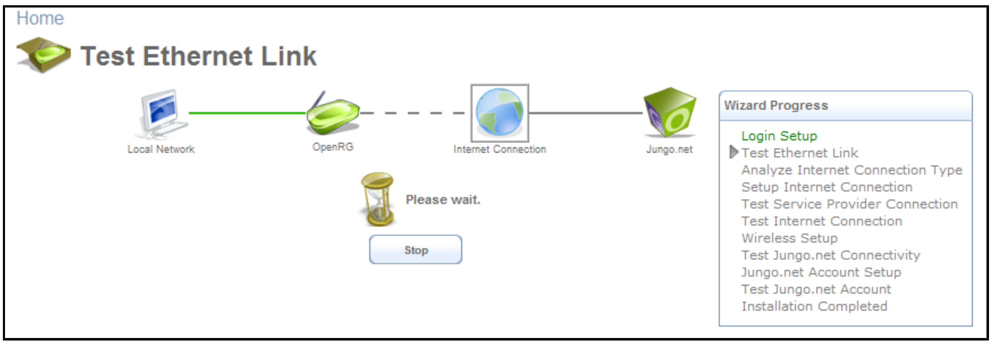


Figure 2.17 Test Ethernet Link

This step may fail if OpenRG cannot detect your Ethernet link (for example, if the cable is unplugged). In this case, the screen changes to the following.

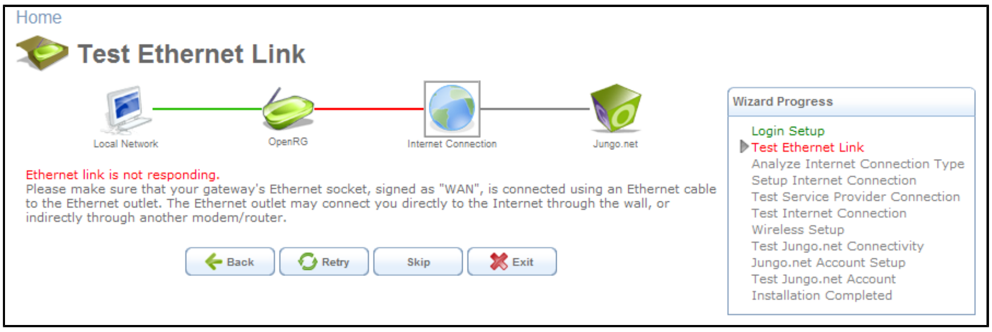


Figure 2.18 Test Ethernet Link – Failure

Verify that your Ethernet/DSL cable is connected properly, and click 'Retry'.

2.3.2 Step 2: Analyze Internet Connection Type

The next step is an analysis of your Internet connection.

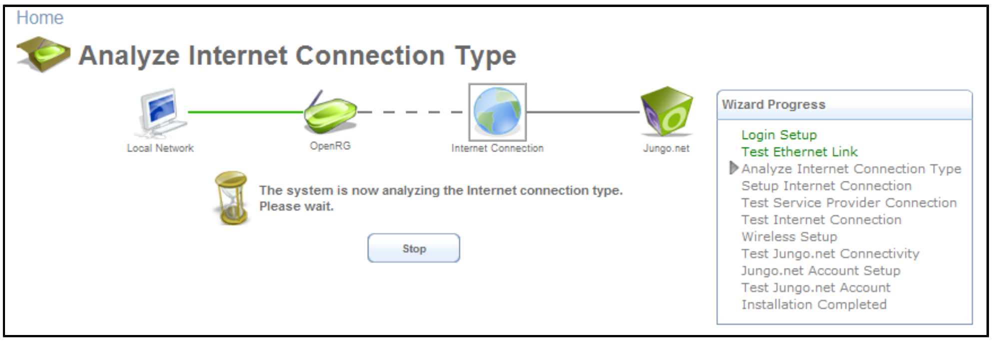


Figure 2.19 Analyze Internet Connection Type

This step may fail if OpenRG is unable to detect your Internet connection type.

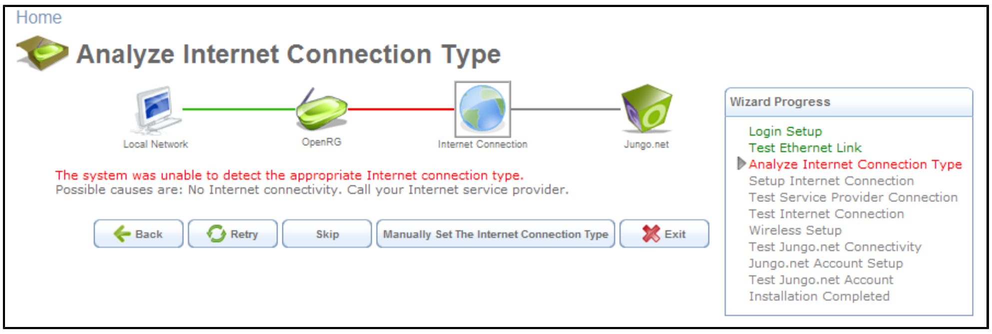


Figure 2.20 Analyze Internet Connection Type – Failure

In this case, you can manually set the Internet connection type, by clicking the corresponding button. The following screen appears.

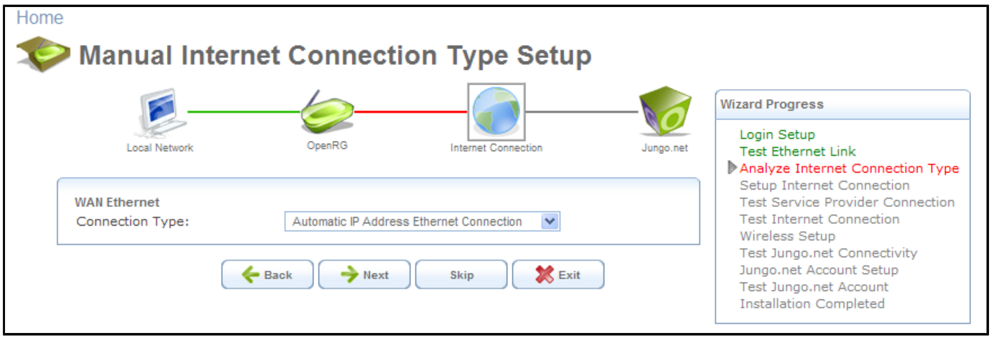


Figure 2.21 Manual Internet Connection Type Setup

To learn about manually configuring your Internet connection, refer to Section 6.4.

2.3.3 Step 3: Setup Internet Connection

If your Internet connection requires login details provided by your Internet Service Provider (ISP) (e.g. when using PPPoE), the following screen appears.

Figure 2.22 Internet Account Information

Enter your user name and password and click 'Next'. Failure to enter the correct details yields the following message. Click 'Back' and try again.

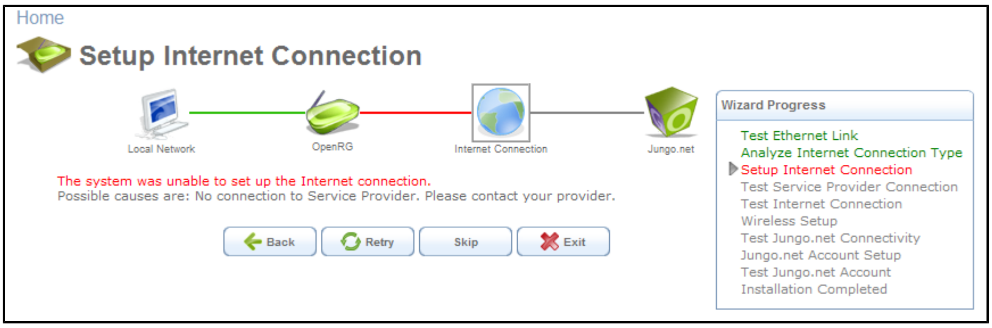


Figure 2.23 Setup Internet Connection

You may have forgotten your login details, issued by your ISP. OpenRG saves the username and password of the PPPoE or PPPoA connection to the ISP, even if it is restored to the factory default settings. When restoring the connection with the installation wizard, OpenRG will offer your old login details.

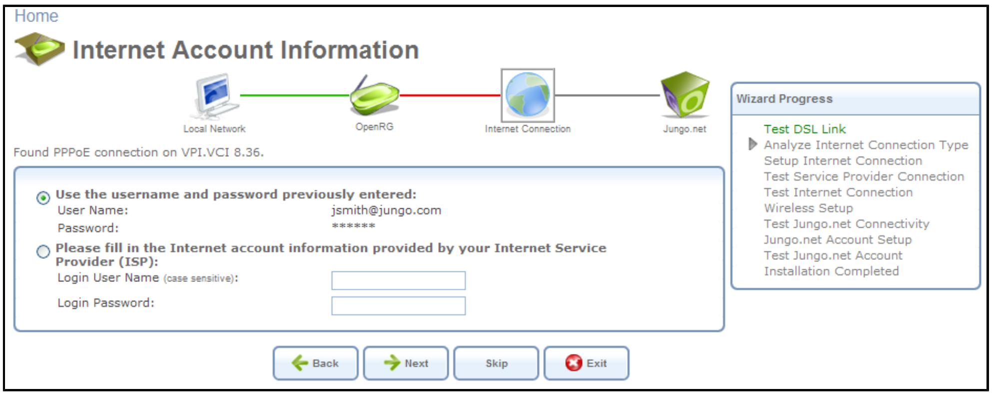


Figure 2.24 Internet Account Information

2.3.4 Step 4: Test Service Provider Connection

This step tests the connectivity to your ISP.

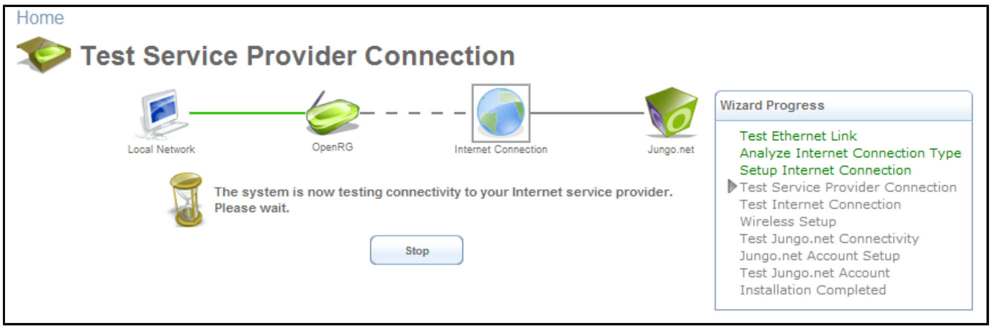


Figure 2.25 Test Service Provider Connection

2.3.5 Step 5: Test Internet Connection

This step tests the connectivity to the Internet.

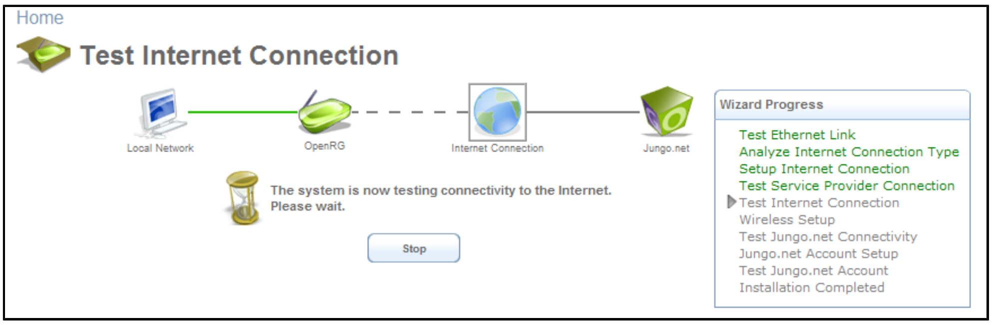


Figure 2.26 Test Internet Connection

2.3.6 Step 6: Wireless Setup

This step enables you to rename your wireless network, as well as change its security level.

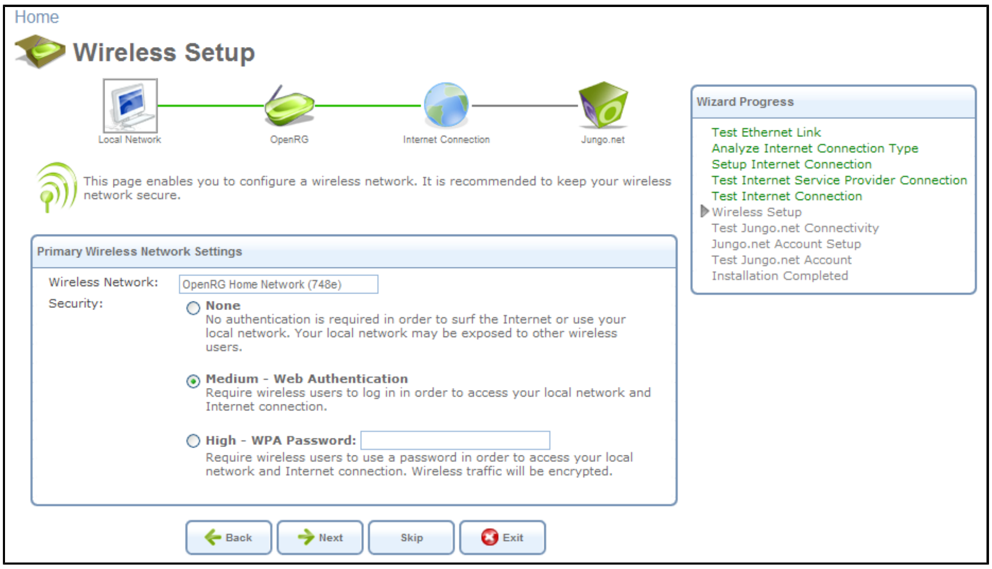


Figure 2.27 Wireless Setup

OpenRG assigns a default name for its wireless network, which you may later change. Select the wireless security level. The default "Medium" level secures your network by requiring users to provide a password in order to connect. "High" level utilizes the Wi-Fi Protected Access (WPA) protocol, requiring a password (network key) as well, but also encrypts the wireless traffic. When selecting this option, enter an eight-character password in the provided field. Click 'Next' to continue.

2.3.6.1 Setup via Wireless Connection

If you are running the installation wizard while being connected to OpenRG via a wireless connection, the wizard does not change the default SSID (to prevent you from disconnecting). If you choose to change it manually, the following screen appears, requesting that you re-establish your wireless connection (from your computer) before proceeding with the wizard.

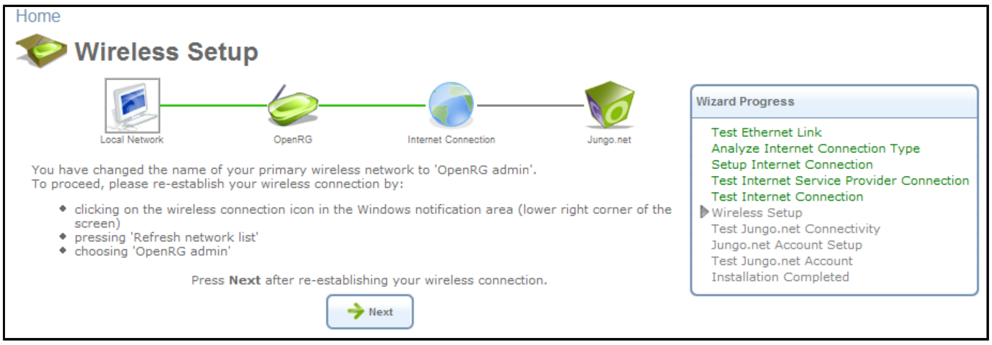


Figure 2.28 Wireless Setup

This screen also appears after selecting the High wireless security level, or after changing the previously entered WPA password (see Figure 2.27).

2.3.6.2 Additional SSIDs with Virtual Access Points

If your gateway supports multiple virtual access points, an additional pre-configured WPA-secured wireless network is displayed in 'Wireless Setup' screen.

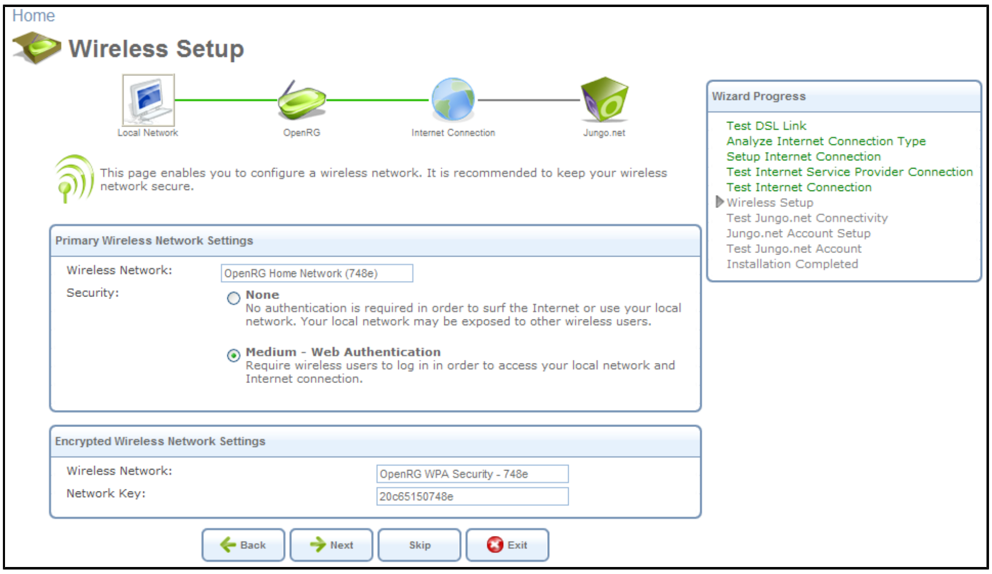


Figure 2.29 Wireless Setup

You can change the default name and network key (password) of this encrypted wireless network in their respective text fields (clicking 'Next' will save the new details). This wireless network will also appear in the 'Network Connections' screen under the 'System' tab, where it can be edited or deleted such as any other network connection.

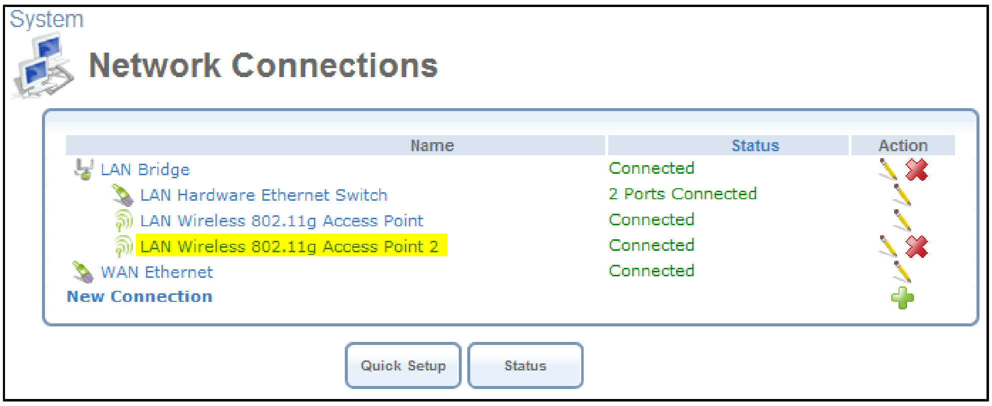


Figure 2.30 Network Connections

Note: In order to delete this connection, you must first remove it from under the LAN bridge.

2.3.7 Step 10: Installation Completed

This screen provides a summary of all the above Internet connection configuration steps and their results. Click 'Finish' to complete the wizard procedure.

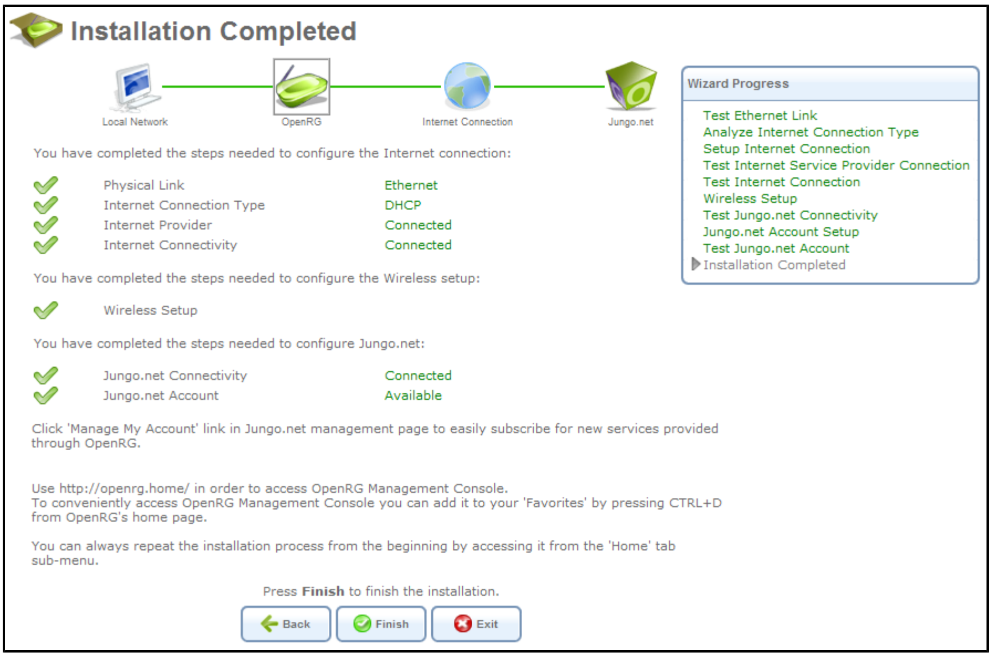


Figure 2.31 Installation Completed

2.4 Configuring Your Wireless Network

The 'Wireless' menu item enables you to view and configure the gateway's 'Home Network' and 'Secured Wireless Network' wireless access points (the rest can only be configured as described in Section 4.3).

Figure 2.32 Settings – Wireless

The first 'Enable Wireless' check box displayed in this screen enables you to activate or deactivate the gateway's entire wireless interface. The 'Home Network' and 'Secured Wireless Network' access points are activate by default. You can change their network names (also known as SSIDs) in the respective name fields.

Both access points are secured with a default password (by default "wlpass123"), which you can change in the 'Global Wireless Password' field. However, the 'Secured Wireless Network' can also be configured with the Wired Equivalent Privacy (WEP) protocol. WEP is a data

encryption method utilizing a 13-character security key that is used for authentication of wireless clients. To utilize WEP, select 'WEP Wireless Network' from the drop-down menu. The screen refreshes, displaying the 'Wireless Password' field, which enables you to define the access point's WEP security key.

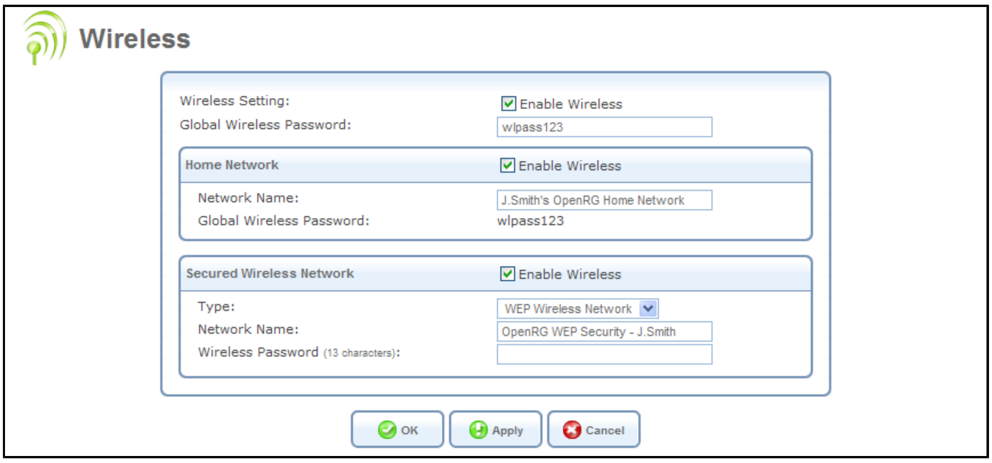


Figure 2.33 Wireless – WEP Security

Enter your personalized security key, and click 'Apply' to save the settings.

3

Internet Connection

3.1 Viewing Your Internet Connection Properties

The 'Overview' screen provides general information regarding your Internet connection, such as the connection's status, protocol, speed, duration, as well as the gateway's external IP address and networking parameters. You can use this screen to quickly view your Internet connection status.

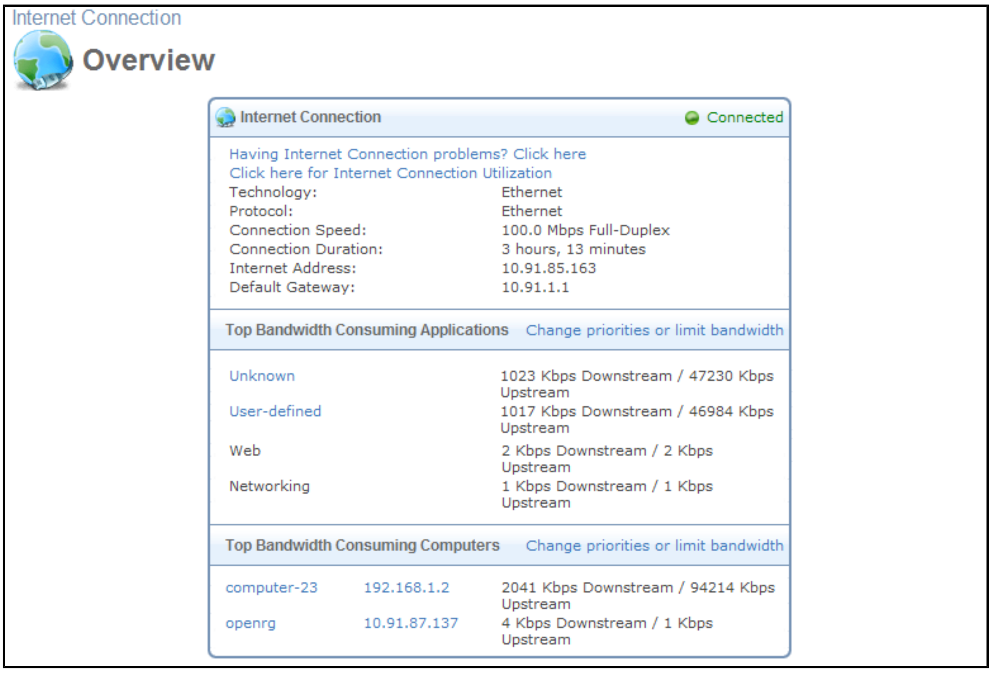


Figure 3.1 Internet Connection – Overview

The following links are available:

- **Have Internet Connection problems? Click here** This link routes you to the 'Troubleshoot' screen, where you can run tests in order to diagnose and resolve Internet connectivity problems.
- **Click Here For Internet Connection Utilization** Click this link to analyze the traffic usage of your WAN connection (for more information, refer to Section 5.3).

In addition, this screen displays OpenRG's top bandwidth consuming applications and computers, described in Section 5.3.2.

3.2 Configuring Your Internet Connection

The 'Settings' screen provides basic configuration options for the different types of Internet connections supported by OpenRG.

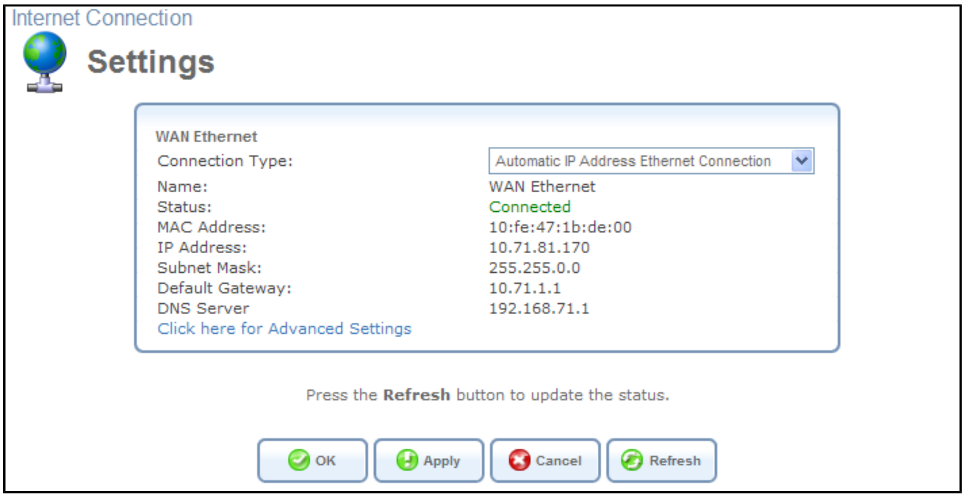


Figure 3.2 Internet Connection – Settings

If you are already connected to the Internet, this screen provides information on your connection. The drop-down menu provides the WAN connection types supported by OpenRG. Each option in this drop-down menu is described thoroughly in Section 6.4.

Click the 'Click here for Advanced Settings' link at anytime to navigate to your WAN connection's properties page. The 'WAN Ethernet Properties' screen appears.

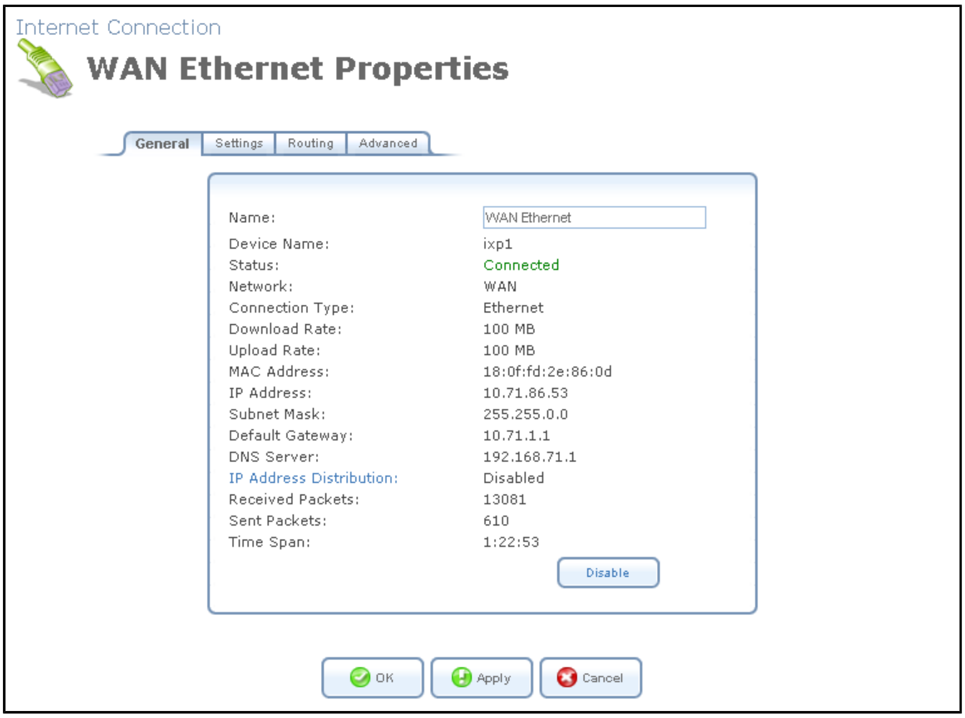


Figure 3.3 WAN Ethernet Properties

This screen provides all the configuration options for your WAN connection. For more information, refer to Section 6.4.7.

4

Local Network

4.1 Overviewing Your Local Network

The 'Overview' screen presents OpenRG's network summary. This includes all connected devices: computers, disks, and phones. When this screen is loaded, OpenRG begins the process of automatically detecting the network services available on connected computers (hosts). The screen then refreshes, displaying each computer's network services.

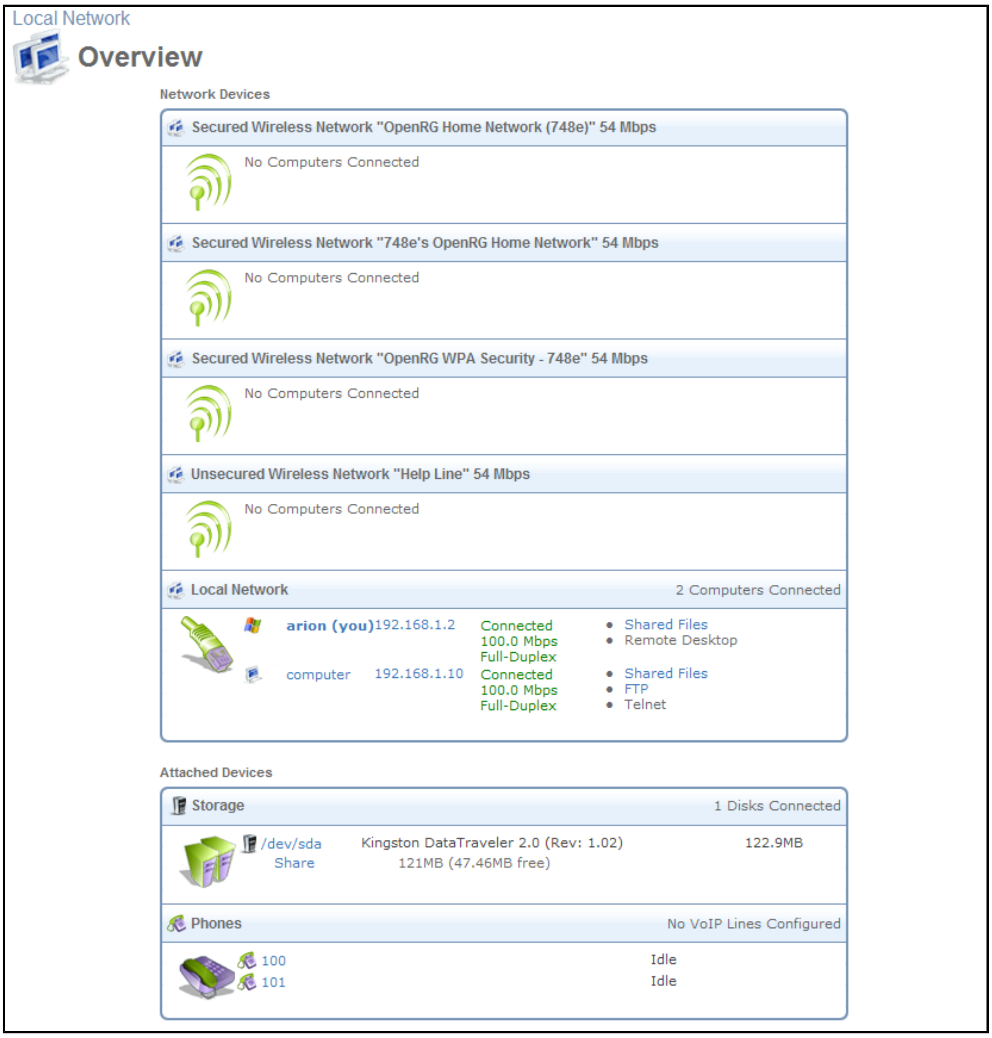


Figure 4.1 Local Network Overview

To view more information on a specific computer, click its respective link. The 'Host Information' screen appears.

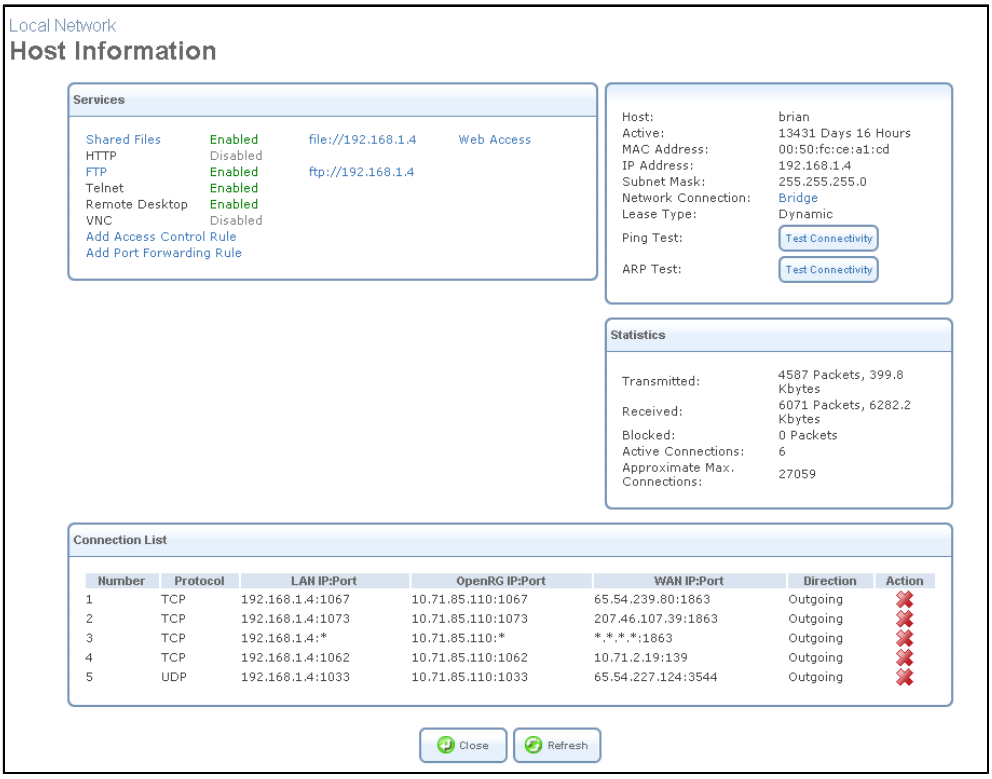


Figure 4.2 Host Information

This screen presents all information that is relevant to the connected computer, such as connection settings, available services, traffic statistics, and connection list. It also enables you to perform connectivity tests with the computer.

Services This section lists the services enabled on the computer that are available to other computers in the LAN, via Web access (SSL-VPN), or from both. Services available via SSL-VPN require a secure (HTTPS) connection (for more information, refer to Section 5.8.2). When a service is accessible from the LAN, you can activate it by either clicking its name or the URL that appears (see Figure 4.2). When a service is accessible via Web access, you can activate it by clicking the 'Web Access' link that appears. Available services are:

- **Shared Files** Access the computer's shared files directory.
- **HTTP** Access the computer's HTTP server (if available).
- **FTP** Open an FTP session with the computer.
- **Telnet** Open a Telnet session with the computer.
- **Remote Desktop** Remotely control a Windows computer with the Remote Desktop utility.
- **VNC** Remotely control the computer with the Virtual Network Computing desktop protocol.
- **Add Access Control Rule** Block access to Internet services from the computer, or allow access if the firewall is set to a "High" security level (for more information, refer to Section 5.2.2).

- **Add Port Forwarding Rule** Expose services on the computer to external Internet users (for more information, refer to Section 5.2.3).

Connection Information This section displays various details regarding the computer's connection settings. In addition, you can run a Ping or ARP test by clicking the respective 'Test Connectivity' button. The tests are performed in the 'Diagnostics' screen (refer to Section 6.8.7).

Statistics This section displays the computer's traffic statistics, such as the number and size of transmitted and received packets.

Connection List This section displays the list of connections opened by the computer on OpenRG's firewall. The table displays the computer's source LAN IP address and port, the gateway's IP address and port to which it is translated, and the destination WAN IP address and port.

4.2 Viewing the Gateway's LAN Devices

The 'Device' screen (see Figure 4.3) presents a summary of OpenRG's LAN devices, including a bridge (if one exists), Ethernet, USB and wireless, and the status of each one (connected/ disconnected).

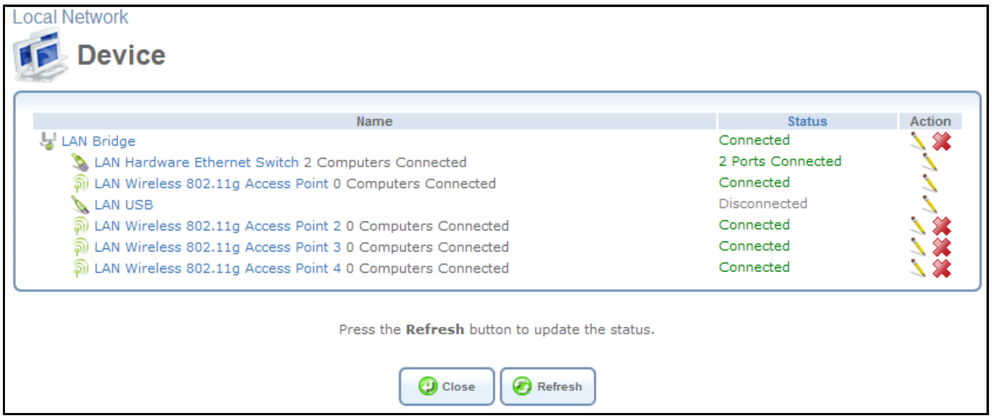


Figure 4.3 Local Network Device View

4.3 Configuring Your Wireless Connection

The 'Wireless' menu item concentrates the wireless LAN settings of your gateway. This screen presents OpenRG's wireless connection settings, and enables you to change them according to your needs.

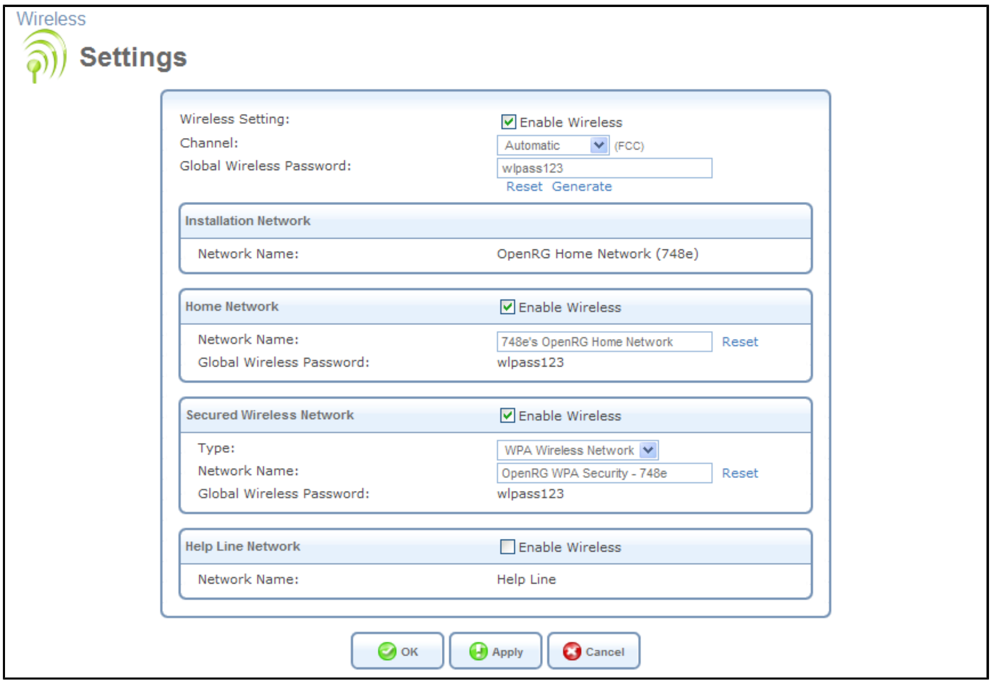


Figure 4.4 Wireless Overview

Enable Wireless Select or deselect this check box to enable or disable the wireless interface.

Channel All devices in your wireless network broadcast on different channels. Leaving this parameter on Automatic ensures that OpenRG continuously scans for the most available wireless channel in your area. It is possible to select a channel manually if you have information regarding the wireless channels used in your vicinity. The channels available depend on the regulatory authority (stated in brackets) to which your gateway conforms. For example, the European regulatory authority (ETSI) has allocated 13 available channels, while the US regulatory authority (FCC) has allocated 11 available channels.

Network Name (SSID) The SSID is the network name shared among all points in a wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). For added security, you may change the default SSID to a unique name.

SSID Broadcast By default, OpenRG broadcasts the name of its wireless network (SSID). For security reasons, you may choose to hide your wireless network by deselecting this check box. Wireless clients will only be able to connect by manually typing the SSID in their wireless client applications (whether Windows or a third party application), rather than choosing it from the list of available wireless networks.

802.11 Mode Select the desired wireless connection type. By default, it is set to 802.11g/n. Note that 802.11b legacy devices are not compatible with modes 802.11g/n and 802.11g Only.

Security Use this section to configure your wireless security settings. Select the type of security protocol from the corresponding drop-down menu. The screen refreshes, presenting each protocol's configuration respectively.

- **WPA** – a data encryption method for 802.11 wireless LANs.

Authentication Method Select the authentication method you would like to use. You can choose between Pre-Shared Key and 802.1x.

Pre-Shared Key This entry appears only if you had selected this authentication method. Enter your encryption key in the 'Pre-Shared Key' field. You can use either an ASCII or a Hex value by selecting the value type in the drop-down menu provided.

Encryption Algorithm Select between Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) for the encryption algorithm, or both of them.

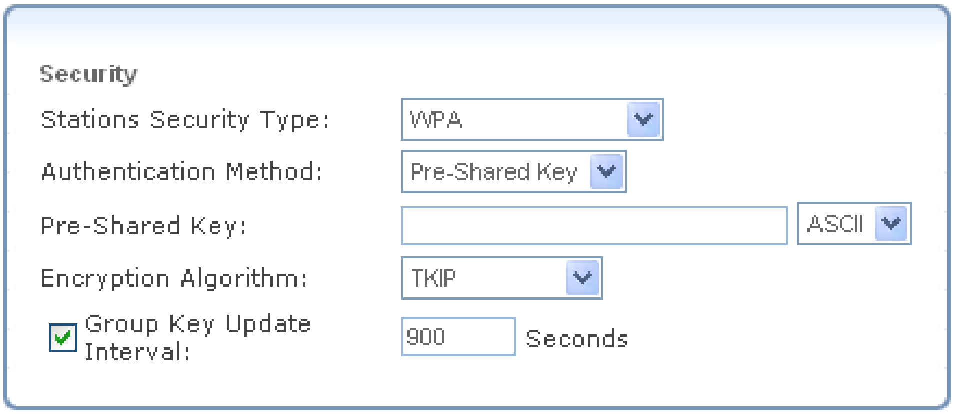


Figure 4.5 WPA Wireless Security Parameters

- **WPA2** – an enhanced version of WPA, and defines the 802.11i protocol.

Authentication Method Select the authentication method you would like to use. You can choose between Pre-Shared Key and 802.1x.

Pre-Shared Key This entry appears only if you had selected this authentication method. Enter your encryption key in the 'Pre-Shared Key' field. You can use either an ASCII or a Hex value by selecting the value type in the drop-down menu provided.

Encryption Algorithm The encryption algorithm used with WPA2 is the AES only.

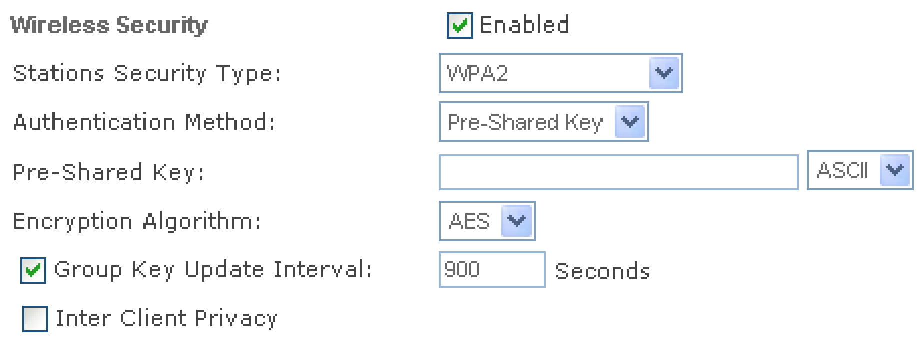


Figure 4.6 WPA2 Wireless Security Parameters

- **WPA and WPA2** – a mixed data encryption method, which utilizes both WPA and WPA2.

Authentication Method Select the authentication method you would like to use. You can choose between Pre-Shared Key and 802.1x.

Pre-Shared Key This entry appears only if you had selected this authentication method. Enter your encryption key in the 'Pre-Shared Key' field. You can use either an ASCII or a Hex value by selecting the value type in the drop-down menu provided.

Encryption Algorithm The encryption algorithm used for WPA and WPA2 is either the AES only, or both AES and TKIP.

Wireless Password The wireless password required to connect to the gateway's wireless network. You may change the default password by either clicking 'Generate' or entering an 8 character long password, and clicking 'Apply'. Note that clicking 'Reset' will return the gateway's default password.

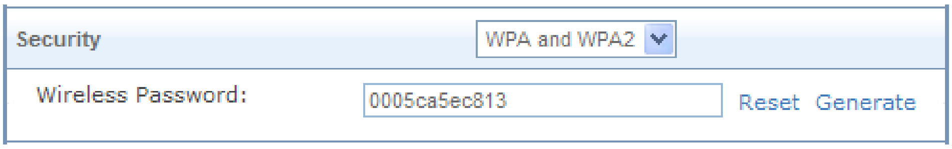


Figure 4.7 WPA and WPA2

- **WEP** – a data encryption method utilizing a statically defined key as the wireless password. Note that the static key must be defined in the wireless Windows client as well, as described below.

Active Select the encryption key to be activated.

Key Length Select the key length in bits: 40 or 104 bits.

Encryption Key Type Select the character type for the key: ASCII or HEX.

Wireless Password Enter the wireless password required to connect to the gateway's wireless network.

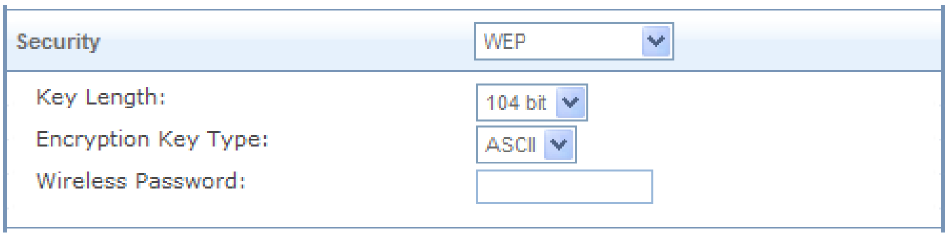


Figure 4.8 WEP

The encryption key (wireless password) must be defined in the wireless Windows computer as well. This is done in the 'Connection Properties Configuration' window:

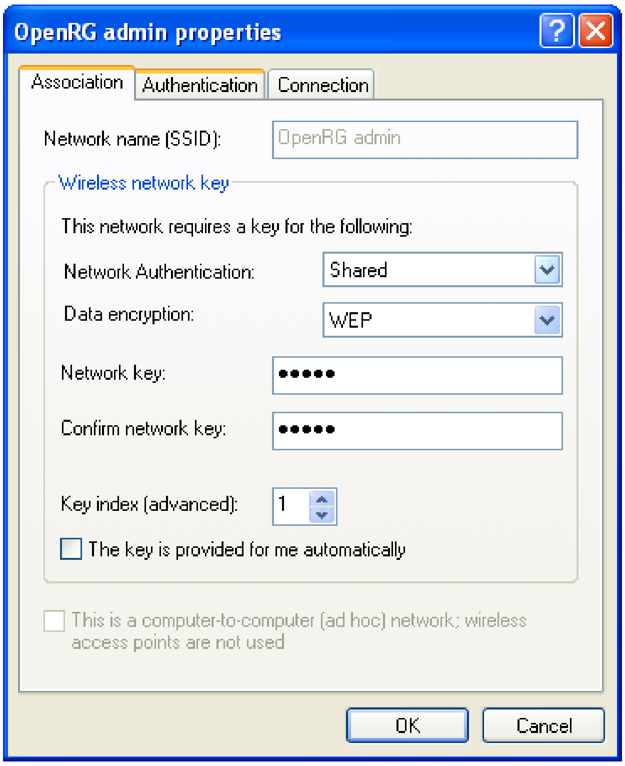


Figure 4.9 Connection Properties Configuration

1. In the 'Network Authentication' drop-down menu, select "Shared".
2. In the 'Data Encryption' drop-down menu, select "WEP".
3. Enter your encryption key in both the 'Network key' and the 'Confirm network key' fields.

- **Unsecured** Selecting this option disables security on your wireless connection. Any wireless computer in your area will be able to connect to the Internet using your connection's bandwidth.

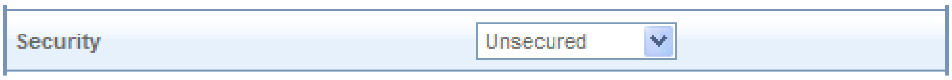


Figure 4.10 Disabled Wireless Security

- **Authentication Only** When selecting this option, wireless clients attempting to connect to the wireless connection will receive OpenRG's main login screen, along with the following attention message:

Figure 4.11 Web Authentication Needed

By logging into the WBM, clients authenticate themselves and are then able to use the connection. OpenRG keeps record of authenticated clients. To clear this list, click the 'Clean Mac List' button. Clients will have to re-authenticate themselves in order to use the wireless connection.

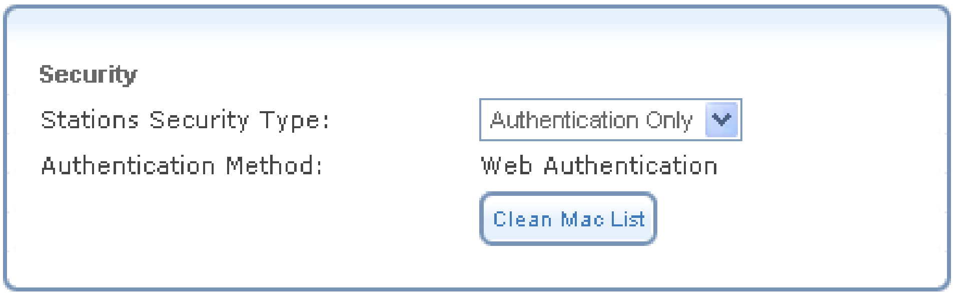


Figure 4.12 Authentication Only Wireless Security Parameters

Wi-Fi Protected Setup (WPS) WPS is a method for simplifying the security setup and management of wireless networks.

Status Indicates the WPS status. "Ready" means that the system is ready to negotiate with incoming wireless clients, or "enrollees".

Protected Setup Method OpenRG supports two setup methods, "Push Button" (the default) and "Client Pin Code". These are the methods used by wireless clients when seeking an access point.

- **Push Button** – The enrollment is initiated by either pressing a physical button on the wireless client or through its software. After initiating the enrollment, click 'Go' or press the WPS button on the top of the gateway for the devices to establish a connection.
- **Client Pin Code** – The enrollment is initiated by the wireless client's software, which also provides a pin code. To comply with this method, select this option from the drop-down menu. The screen refreshes to provide a field for entering the pin code:

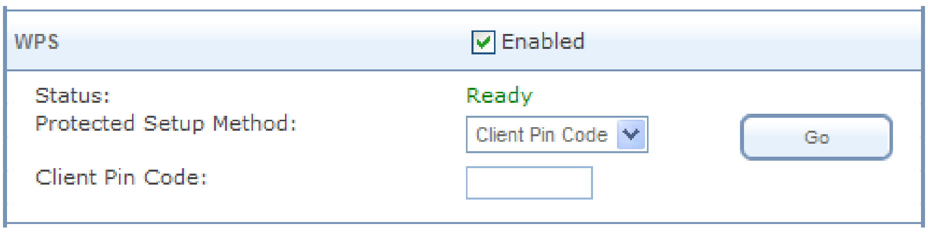


Figure 4.13 Protected Setup Method – Pin Code

In this field, enter the eight digit pin code provided by the wireless client's software. Click 'Go' for the devices to establish a connection.

When attempting to connect a wireless client to OpenRG, you must be aware of its setup method. A connection attempt will time out after two minutes if no connection is established. If a connection is established, the 'Status' field will change to reflect that.

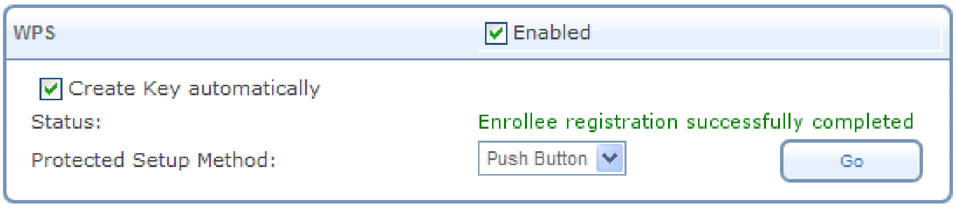


Figure 4.14 Successful Enrollee Registration

Note that WPS is only supported with WPA security. Therefore, when 'WEP' or 'Unsecured' are selected in the 'Security' drop-down menu, the following message appears in the WPS section.

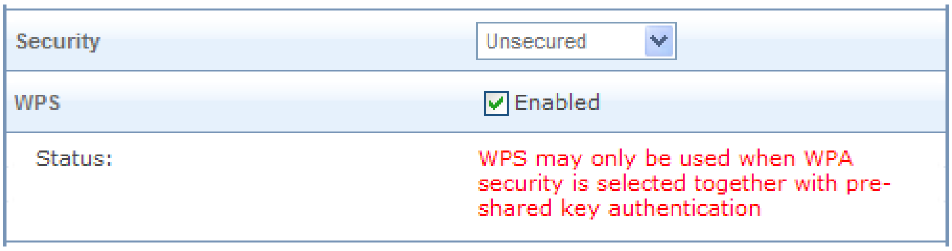


Figure 4.15 WPS Not Supported

MAC Filtering You can filter wireless clients according to their MAC addresses, either allowing or denying them access to your wireless network. To add a MAC filtering rule, choose the action to be performed (allow or deny) in the drop-down menu. Then, click 'New MAC Address'. The 'MAC Filtering Settings' screen appears.

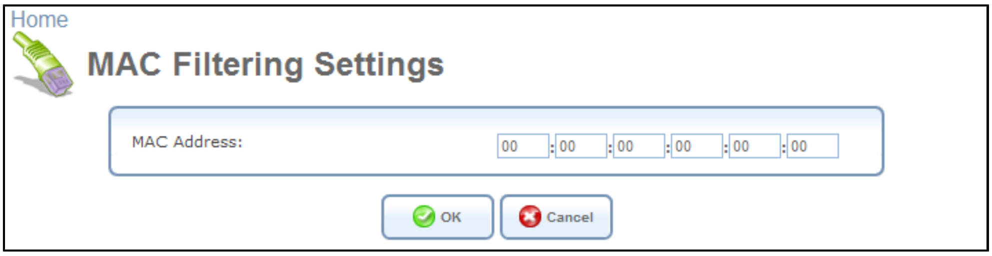


Figure 4.16 MAC Filtering Settings

Enter the MAC address (in hexadecimal values) to be filtered and click 'OK'. The MAC address entry appears.

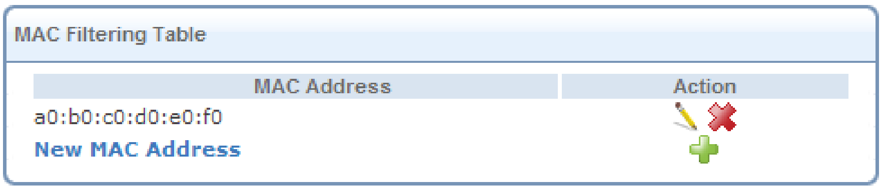


Figure 4.17 MAC Filtering Entry

Note that when 'Allow' is selected, only wireless clients listed in this table will be able to connect. When 'Deny' is selected, all *but* wireless clients listed will be able to connect.

4.4 Managing Your Shared Printers

OpenRG includes a print server that enables your LAN users to share printers attached to the gateway via the USB connection. This eliminates the need to physically connect your printer to a dedicated host, which should be shared and always left on. In addition, the print server offers you such advantages as:

- Support for several print protocols, which enable you to connect Windows, Unix and Mac hosts to the network printer.
- Ability to define printer access permissions for specific LAN users.

4.4.1 Configuring the Print Server

Access the print server settings by clicking the 'Shared Printers' menu item under the 'Local Network' tab. The 'Print Server' screen appears, enabling you to manage your network printer.

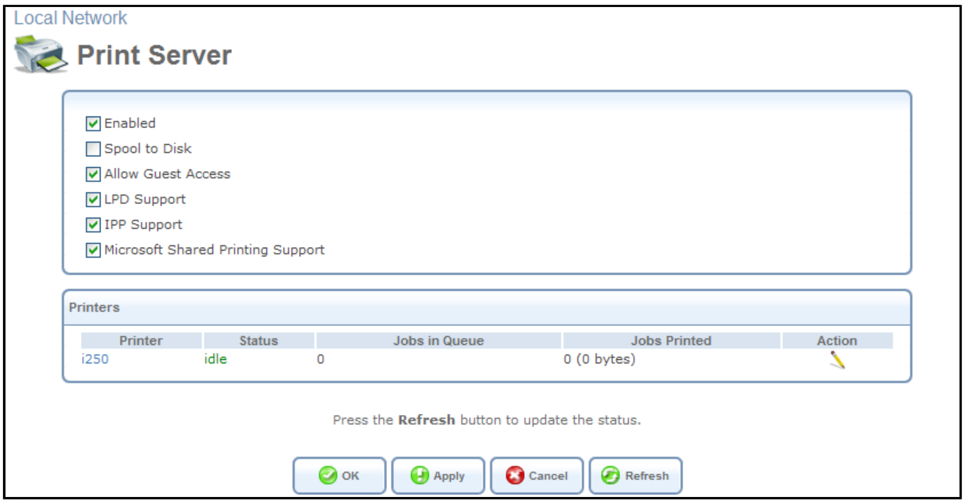


Figure 4.18 Print Server

Enabled Select or deselect this check box to enable or disable this feature.

Spool to Disk Select this check box to temporarily store your print jobs on the disk share, until they are finished. This is especially useful if you would like the printer to process the print job even after you turn the computer off.

The 'Printers' section of this screen displays the printer(s) connected to OpenRG, the device status, and print job information. Click a printer's name link to view its details. The 'Printer' screen appears.

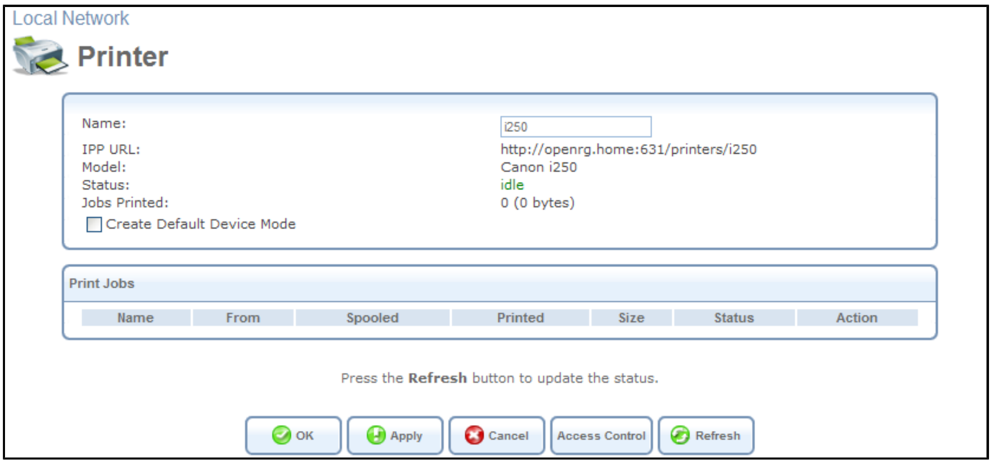


Figure 4.19 Connected Printer

4.5 Managing Your Private Telephony Switching System

The 'IP-PBX' menu item is available on the OpenSMB gateway only. It presents the main screen of the Internet Protocol Private Branch Exchange (IP-PBX) feature, displaying the SIP extensions available on your gateway.

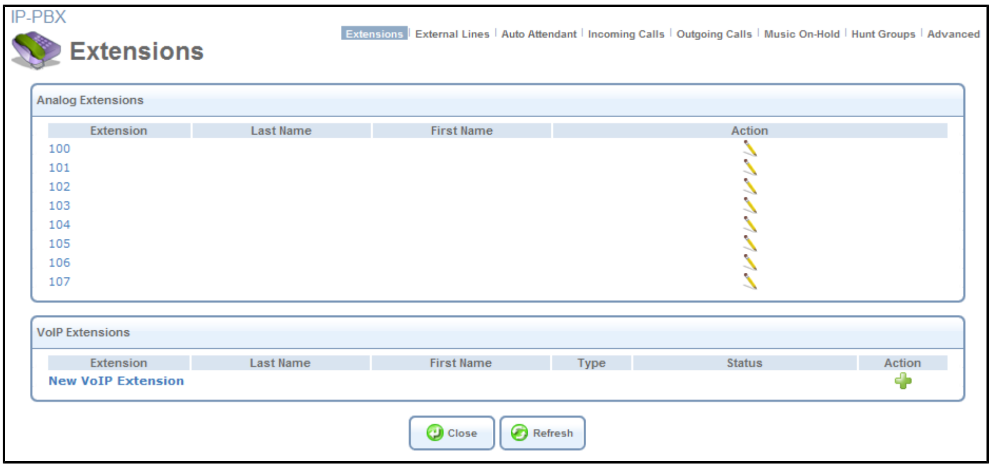


Figure 4.20 IP-PBX Lines

For more information about the IP-PBX feature, refer to Section 5.6.

5

Services

5.1 Overviewing Your Services

The 'Overview' screen presents a summary of OpenRG's services and their current status (enabled/disabled). These services are configurable via their respective menu items under the 'Services' tab.

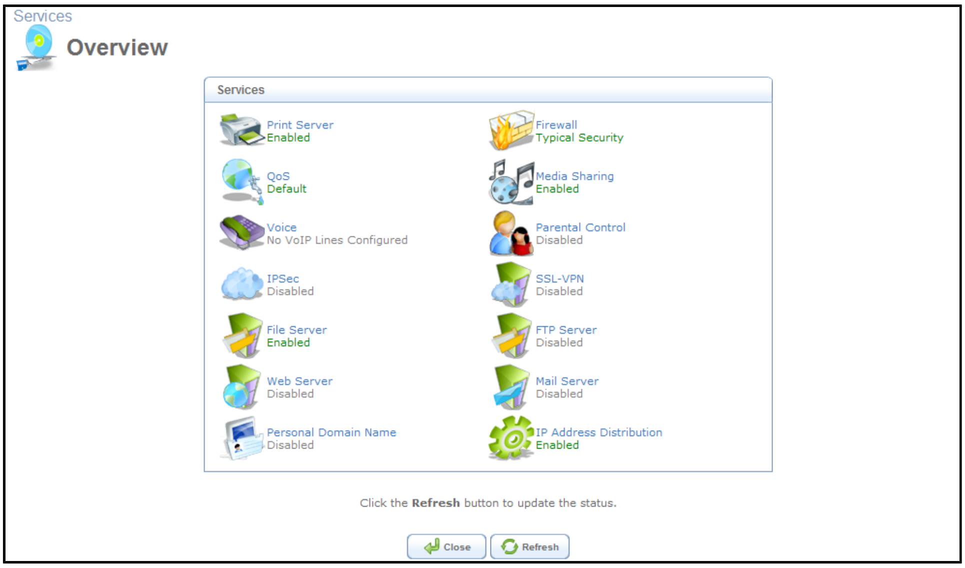


Figure 5.1 Services Overview

5.2 Securing Your Network with the Firewall

OpenRG's gateway security suite includes comprehensive and robust security services: Stateful Packet Inspection Firewall, user authentication protocols and password protection mechanisms. These features together allow users to connect their computers to the Internet and simultaneously be protected from the security threats of the Internet. The firewall, RG-FW OpenRG™, the cornerstone of your gateway's security suite, has been exclusively tailored to the needs of the residential/office user and has been pre-configured to provide optimum security (see Figure 5.2).

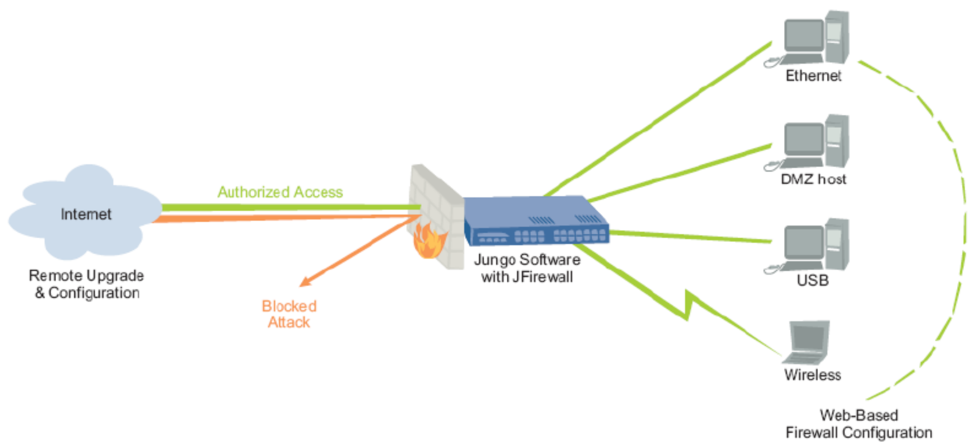


Figure 5.2 OpenRG's Firewall in Action

OpenRG's firewall provides both the security and flexibility that home and office users seek. It provides a managed, professional level of network security while enabling the safe use of interactive applications, such as Internet gaming and video-conferencing.

Additional features, including browsing restrictions and access control, can also be easily configured locally by the user through a user-friendly Web-based interface, or remotely by a service provider. The OpenRG firewall supports advanced filtering, designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN network devices.

5.2.1 Configuring Basic Security Settings

The 'General' screen enables you to configure the gateway's basic security settings.

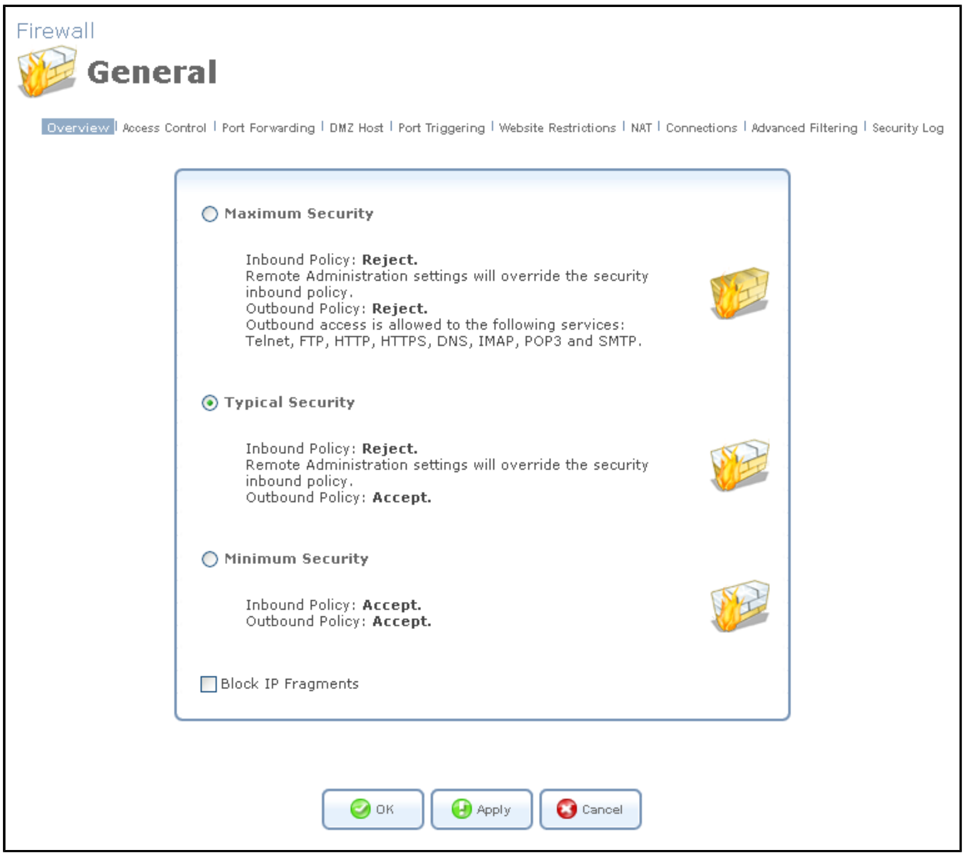


Figure 5.3 General

You may choose between three pre-defined security levels for OpenRG: Minimum, Typical (the default), and Maximum. The following table summarizes OpenRG's behavior for each of the three security levels.

Security Level	Requests Originating in the WAN (Incoming Traffic)	Requests Originating in the LAN (Outgoing Traffic)
Maximum Security	*Blocked*: No access to home network from Internet, except as configured in the Port Forwarding, DMZ host and Remote Access screens	*Limited*: Only commonly-used services, such as Web-browsing and e-mail, are permitted. The list of allowed services can be edited in the Access Control screen (refer to Section 5.2.2)
Typical Security (Default)	*Blocked*: No access to home network from Internet, except as configured in the Port Forwarding, DMZ host and Remote Access screens	*Unrestricted*: All services are permitted, except as configured in the Access Control screen

Minimum Security	*Unrestricted*: Permits full access from Internet to home network; all connection attempts permitted	*Unrestricted*: All services are permitted, except as configured in the Access Control screen

Table 5.1 OpenRG's Firewall Security Levels

To configure OpenRG's basic security settings, perform the following:

1. Choose between the three predefined security levels described in the table above.

   Note: Using the *Minimum Security* setting may expose the home network to significant security risks, and thus should only be used, when necessary, for short periods of time.

2. Check the 'Block IP Fragments' box in order to protect your home network from a common type of hacker attack that could make use of fragmented data packets to sabotage your home network. Note that VPN over IPSec and some UDP-based services make legitimate use of IP fragments. In case of enabling these services, you will need to allow IP fragments to pass into the home network.

3. Click 'OK' to save the settings.

By default, the selected security level is applied on such services as Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SNTP. Note that some applications (such as some Internet messengers and Peer-To-Peer client applications) tend to use ports of the above-mentioned services, if these applications cannot connect using their own default ports. When allowing this behavior, the applications' outbound connection requests will not be blocked, even at the Maximum Security level.

After the security level is set, the firewall regulates the flow of data between the home network and the Internet. Both incoming and outgoing data are inspected and then either accepted (allowed to pass through OpenRG) or rejected (barred from passing through OpenRG), according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside, while allowing home users access to the Internet services that they require.

The firewall rules specify what types of services available on the Internet may be accessed from the home network and what types of services available in the home network may be accessed from the Internet. Each request for a service that the firewall receives, whether originating from the Internet or from a computer in the home network, is checked against the set of firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, then all subsequent data associated with this request (a "session") will also be allowed to pass, regardless of its direction.

For example, when you point your browser to a Web page, a request is sent out to the Internet for retrieving and loading this page. When the request reaches OpenRG, the firewall identifies the request's type and origin—HTTP and a specific PC in your home network, in this case. Unless you have configured access control to block requests of this type from this computer,

the firewall will allow this request to pass out onto the Internet (refer to Section 5.2.2 for more on setting OpenRG's access control).

When the Web page is returned from the Web server, the firewall associates it with this session and allows it to pass, regardless of whether HTTP access from the Internet to the home network is blocked or permitted. It is the *origin of the request*, not the subsequent responses to this request, that determines whether a session can be established or not.

5.2.2 Controlling Access to Internet Services

You may want to block specific computers within the home network (or even the whole network) from accessing certain services on the Internet. For example, you may want to prohibit one computer from browsing the Web, another computer from transferring files using FTP, and the whole network from receiving e-mail (by blocking the *outgoing* requests to POP3 servers on the Internet). The 'Access Control' screen enables you to define restrictions on the types of requests that may pass from the home network out to the Internet, and thus may block traffic flowing in both directions. It can also be used for allowing specific services when maximum security is configured.

- To allow or restrict services:

1. Click 'Access Control' under the 'Firewall' menu item. The 'Access Control' screen appears.

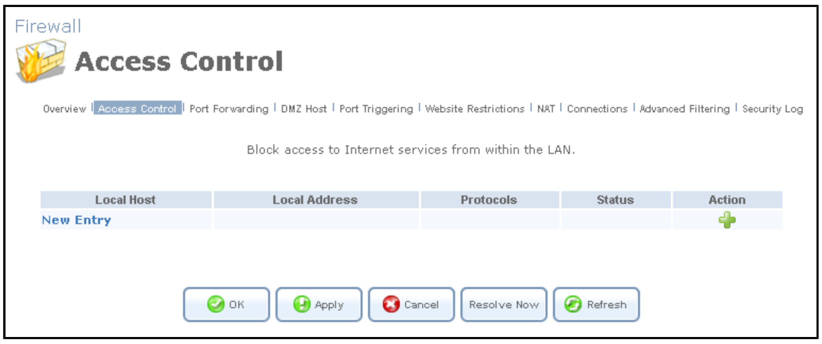


Figure 5.4 Access Control

2. Click the 'New Entry' link. The 'Add Access Control Rule' screen appears.

Figure 5.5 Add Access Control Rule

3. The 'Address' drop-down menu enables you to specify the computer or group of computers on which you would like to apply the access control rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on all OpenRG's LAN hosts. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.

4. The 'Protocol' drop-down menu enables you to select or specify the type of protocol that will be used. Selecting the 'Show All Services' option expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This will commence a sequence that will add a new **Service**, representing the protocol. Refer to Section 6.9.2 in order to learn how to do so.

5. Select the 'Reply an HTML page to the blocked client' check box to display the following message to the client: "Access Denied – this computer is not allowed to surf the WAN. Please contact your admin.". When this check box is deselected, the client's packets are simply ignored and no notification is issued.

6. By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

7. Click 'OK' to save your changes. The 'Access Control' screen displays a summary of the rule that you have just added.

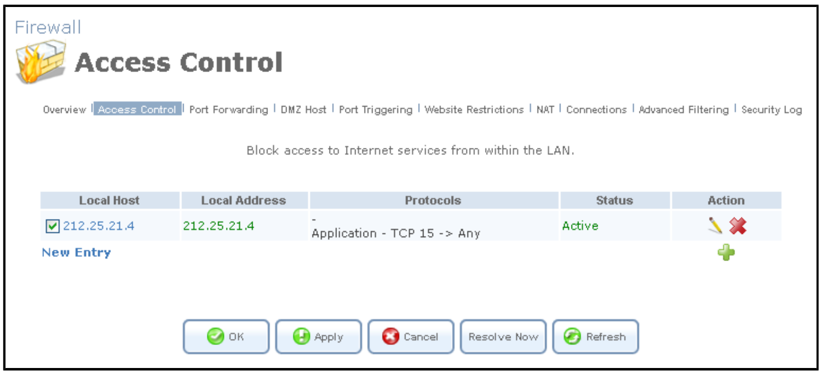


Figure 5.6 Access Control Rule

You may edit the access control rule by modifying its entry displayed under the 'Local Host' column.

- To modify a rule's entry:

    1. Click the rule's action icon . The 'Edit Access Control Rule' screen appears. This screen allows you to edit all the parameters that you configured when creating the access control rule.

Figure 5.7 Edit Access Control Rule

    2. Click 'OK' to save your changes and return to the 'Access Control' screen.

You can disable an access control rule in order to make a service available without having to remove the rule from the 'Access Control' screen. This may be useful if you wish to make the service available only temporarily, intending to reinstate the restriction in the future.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, simply reselect the check box.
- To remove a rule, click the service's action icon . The service will be permanently removed.

When the 'Maximum' security level is applied, the 'Access Control' screen also displays a list of automatically generated firewall rules that allow access to specific Internet services from the LAN computers, over pre-defined ports.

Figure 5.8 Access Control – Allowed Services in Maximum Security Mode

You can manage these access control rules as well as create new ones (allowing access to other services), as described earlier in this section.

> Note: When the Parental Control service is enabled (refer to Section 5.7), HTTP services cannot be blocked by Access Control.

5.2.3 Using Port Forwarding

In its default state, OpenRG blocks all external users from connecting to or communicating with your network. Therefore, the system is safe from hackers who may try to intrude into the network and damage it. However, you may wish to expose your network to the Internet in certain limited and controlled ways. The Port Forwarding feature enables you to do so. If you are familiar with networking terminology and concepts, you may have encountered the port forwarding capability referred to as "Local Servers".

The 'Port Forwarding' screen enables you to define applications (such as Peer-to-Peer, game, voice, chat programs, etc.) that will be allowed a controlled Internet activity. For example,

if you wish to use a File Transfer Protocol (FTP) application on one of your PCs, you would simply create a port forwarding rule, which specifies that all FTP-related data arriving at OpenRG from the Internet will henceforth be forwarded to the specified computer.

Similarly, you can grant Internet users access to servers inside your home network, by identifying each service and the PC that will provide it. This is useful, for example, if you would like to host a Web server inside your home network. When an Internet user points a browser to OpenRG's external IP address, the gateway will forward the incoming HTTP request to your Web server, if the corresponding port forwarding rule had been set.

However, there is a limitation that must be considered. With one external IP address (OpenRG's main IP address), different applications can be assigned to your LAN computers, however each type of application is limited to use one computer. For example, you can define that FTP will use address X to reach computer A and Telnet will also use address X to reach computer A, but attempting to define FTP to use address X to reach both computer A and B will fail. OpenRG therefore provides the ability to add additional public IP addresses to port forwarding rules, which you must first obtain from your ISP, and enter into the 'NAT IP Addresses Pool' (refer to Section 5.2.6). You will then be able to define FTP to use address X to reach computer A, and address Y to reach computer B.

Additionally, port forwarding enables you to redirect traffic to a different port instead of the one for which it was designated. For example, you have a Web server running on your PC on port 8080 and you want to grant access to this server to anyone who accesses OpenRG via HTTP (by default, on port 80). To accomplish this, you will have to define a port forwarding rule for the HTTP service, with the PC's IP or host name, as well as specify 8080 in the 'Forward to Port' field. All incoming HTTP traffic will be forwarded to the PC running the Web server on port 8080.

When setting a port forwarding service, you must ensure that the port is not already in use by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP—the port used by the gateway's VoIP application (5060) is the same port on which port forwarding is set for LAN SIP agents. For more details, refer to Section 5.5.8.3.

Some applications that work with such protocols as FTP, TFTP, PPTP and H.323, require the support of specific Application Level Gateway (ALG) modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. OpenRG is configured with a robust list of ALG rules in order to enable maximum functionality in the home network. These ALG rules are automatically applied based on the destination ports. You may also create additional ALG rules. To learn how to do so, refer to Section 5.2.7.2).

5.2.3.1 Adding a Port Forwarding Rule

To add a new port forwarding rule, perform the following:

1. Click 'Port Forwarding' under the 'Firewall' menu item. The 'Port Forwarding' screen appears.

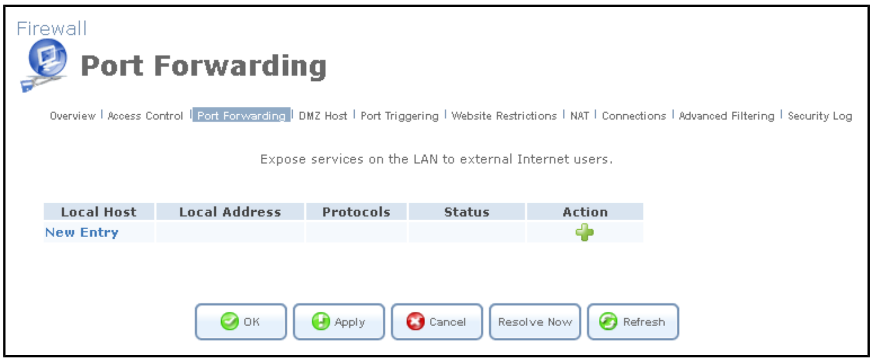


Figure 5.9 Port Forwarding

2. Click the 'New Entry' link. The 'Add Port Forwarding Rule' screen appears.

Figure 5.10 Add Port Forwarding Rule – Basic

3. Click the 'Advanced' button at the bottom of the screen. The screen expands.

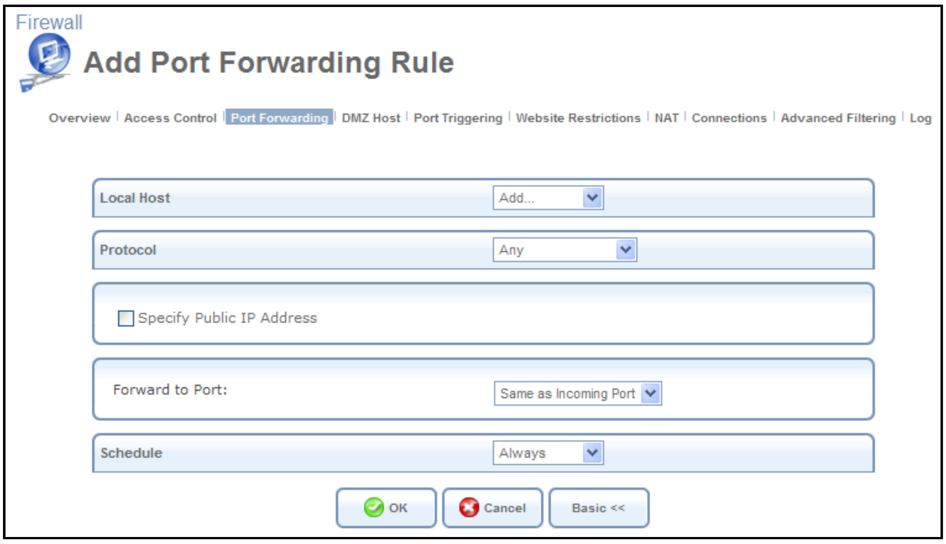


Figure 5.11 Add Port Forwarding Rule – Advanced

4. The 'Local Host' drop-down menu lists your available LAN computers. Select a computer that provides the service, to which you wish to grant access over the Internet. If you would

like to add a new computer, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to Section 6.9.2 in order to learn how to do so. Note that unless an additional external IP address has been added, only one LAN computer can be assigned to provide a specific service or application.

5. The 'Protocol' drop-down menu enables you to select or specify the type of protocol that will be used. Selecting the 'Show All Services' option expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This will commence a sequence that will add a new **Service**, representing the protocol. Refer to Section 6.9.2 in order to learn how to do so.

6. When creating a port forwarding rule, you must ensure that the port used by the selected protocol is not already in use by any other of your local services, which, in this case, may stop functioning. A common example is when using SIP signaling in Voice over IP—the port used by the gateway's VoIP application (5060) is the same port on which port forwarding is set for LAN SIP agents. For more details, refer to Section 5.5.8.3.

7. If you would like to apply this rule on OpenRG's non-default IP address (which you can define in the 'NAT' screen, as described in Section 5.2.6), perform the following:

   a. Select the 'Specify Public IP Address' check box. The screen refreshes.

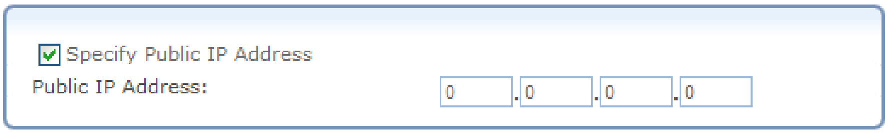


Figure 5.12 Specify Public IP Address

   b. Enter the additional external IP address in the 'Public IP Address' field.

8. By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

9. Click 'OK' to save your changes. The 'Port Forwarding' screen displays a summary of the rule that you have just added.

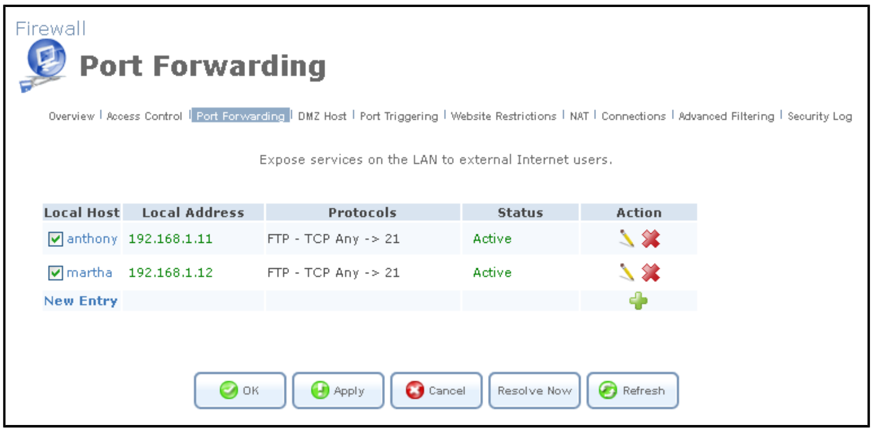


Figure 5.13 Port Forwarding Rule

You may edit the port forwarding rule by clicking its entry under the 'Local Host' column in the 'Port Forwarding' screen. You can also disable the rule in order to make a service unavailable without having to remove the rule from the 'Port Forwarding' screen. This may be useful if you wish to make the service unavailable only temporarily, intending to reinstate it in the future.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, simply reselect the check box.
- To remove a rule, click the service's  action icon . The service will be permanently removed.

All the computers in the local network can simultaneously use a specific service as clients. Being a client means that the computer within the network initiates the connection—for example, opens an FTP connection with an FTP server on the Internet. However, only one computer can serve as a server, responding to requests from computers on the Internet.

5.2.4 Using Port Triggering

Port triggering is used for setting a dynamic port forwarding configuration. By setting port triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. This is called port triggering since the outbound traffic triggers to which ports inbound traffic is directed.

For example, consider a gaming server that is accessed using the UDP protocol on port 2222. The gaming server responds by connecting the user using UDP on port 3333, when starting gaming sessions. In such a case you must use port triggering, since this scenario conflicts with the following default firewall settings:

- The firewall blocks inbound traffic by default.

- The server replies to OpenRG's IP, and the connection is not sent back to your host, since it is not part of a session.

In order to solve this, you need to define a Port Triggering entry, which allows inbound traffic on UDP port 3333 only after a LAN host generated traffic to UDP port 2222. To do so, perform the following:

1. Click the 'Port Triggering' link under the 'Firewall' menu item. The 'Port Triggering' screen appears. This screen will list all of the port triggering entries.

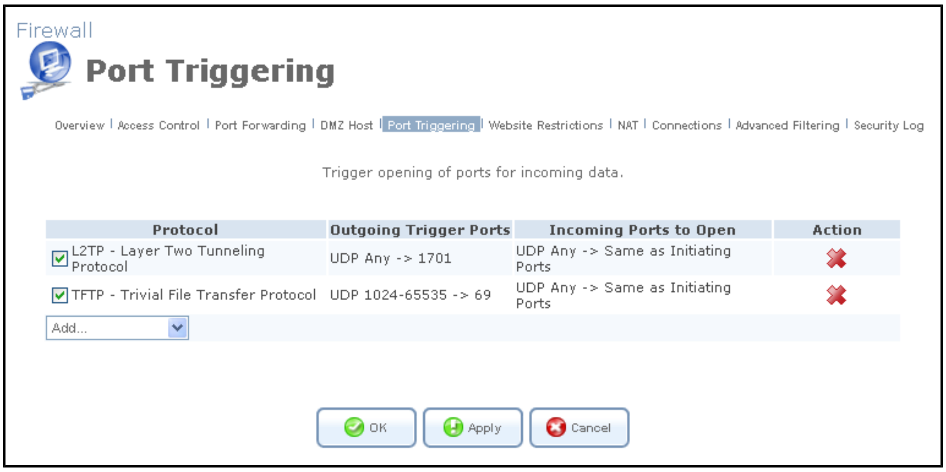


Figure 5.14 Port Triggering

2. Select the 'User Defined' option to add an entry. The 'Edit Port Triggering Rule' screen appears.

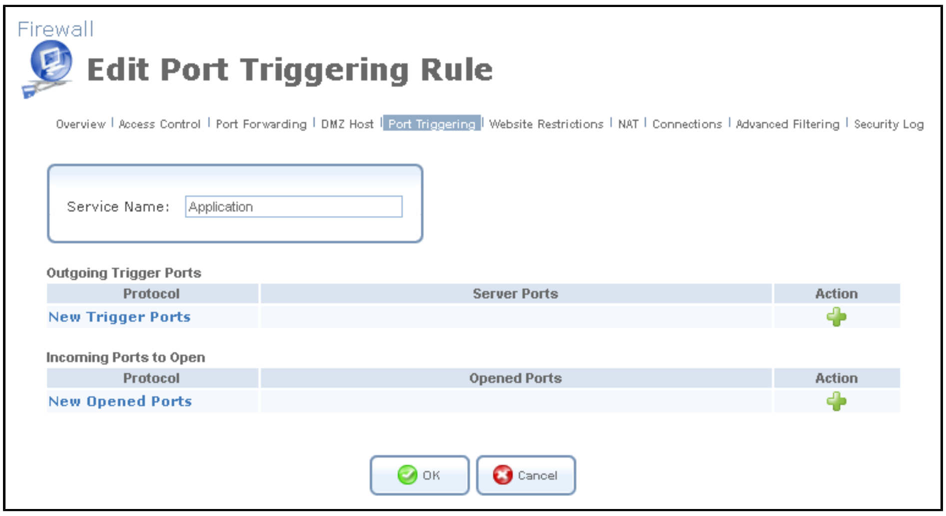


Figure 5.15 Edit Port Triggering Rule

3. Enter a name for the service (e.g. "game_server"), and click the 'New Trigger Ports' link. The 'Edit Service Server Ports' screen appears.

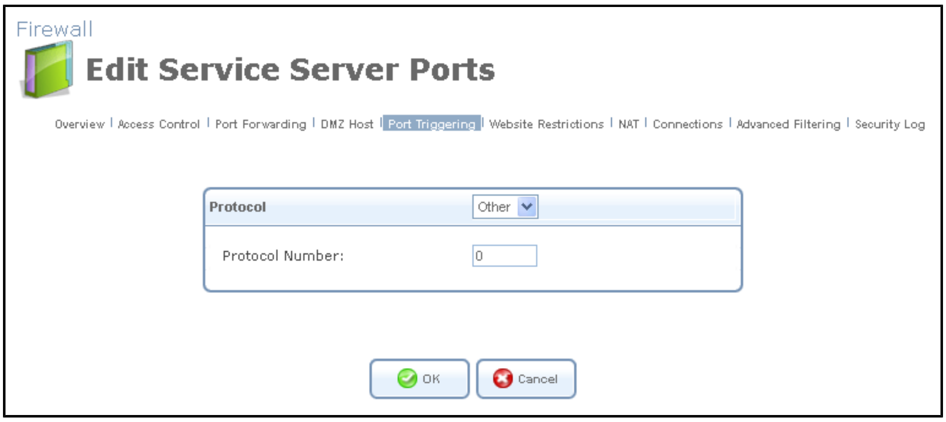


Figure 5.16 Edit Service Server Ports

4. From the 'Protocol' drop-down menu, select 'UDP'. The screen will refresh, providing source and destination port options (see Figure 5.17).

5. Leave the 'Source Ports' drop-down menu at its default "Any". From the 'Destination Ports' drop-down menu, select "Single". The screen will refresh again, providing an additional field in which you should enter "2222" as the destination port.

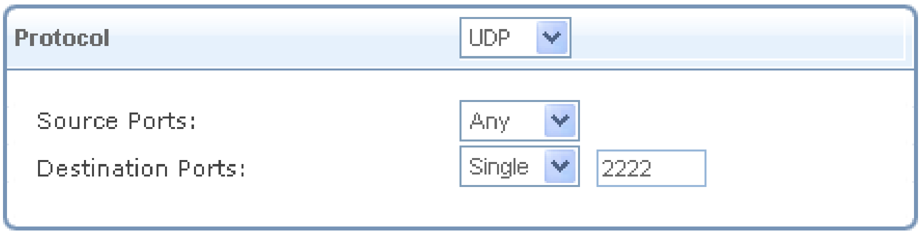


Figure 5.17 Edit Service Server Ports

6. Click 'OK' to save the settings.

7. Back in the 'Edit Port Triggering Rule' screen (see Figure 5.15), click the 'New Opened Ports' link. The 'Edit Service Opened Ports' screen appears.

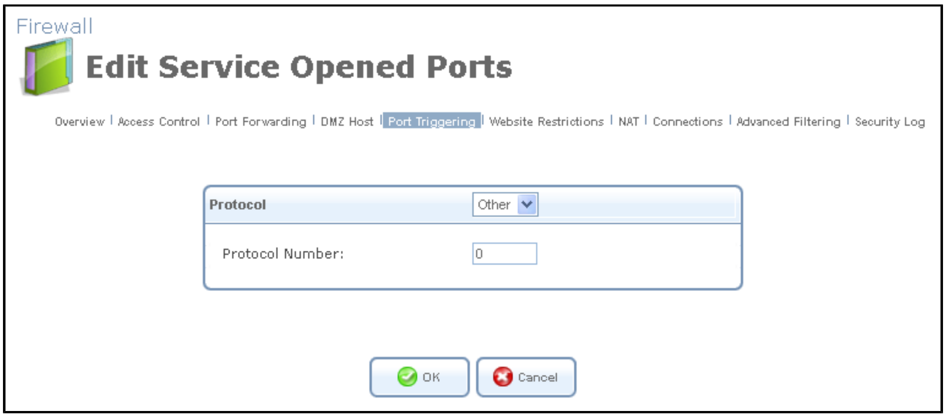


Figure 5.18 Edit Service Opened Ports

8. Select UDP as the protocol, leave the source port at "Any", and enter a 3333 as the single destination port.

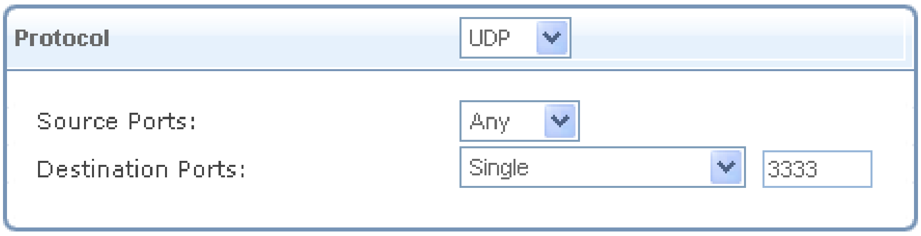
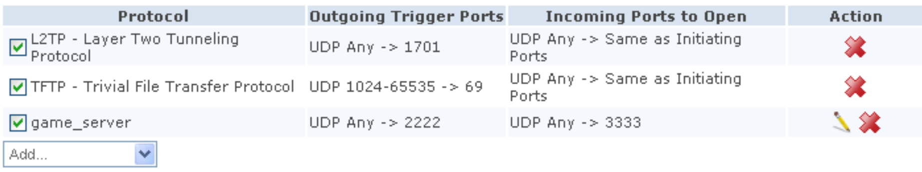


Figure 5.19 Edit Service Opened Ports

9. Click 'OK' to save the settings. The 'Edit Service' screen will present your entered information. Click 'OK' again to save the port triggering rule. The 'Port Triggering' screen will now include the new port triggering entry.



Protocol	Outgoing Trigger Ports	Incoming Ports to Open	Action
L2TP - Layer Two Tunneling Protocol	UDP Any -> 1701	UDP Any -> Same as Initiating Ports	
TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	UDP Any -> Same as Initiating Ports	
game_server	UDP Any -> 2222	UDP Any -> 3333	
Add...			

Figure 5.20 New Port Triggering Rule

This will result in accepting the inbound traffic from the gaming server, and sending it back to the LAN Host which originated the outgoing traffic to UDP port 2222.

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, simply reselect the check box.
- To remove a rule, click the service's action icon . The service will be permanently removed.

> Note: There may be a few default port triggering rules listed when you first access the port triggering screen. Disabling these rules may result in impaired gateway functionality.

5.2.5 Restricting Web Access

You can configure OpenRG to block specific websites so that they cannot be accessed from computers in the home network. Moreover, restrictions can be applied according to a comprehensive and automatically updated list of sites to which access is not recommended.

- To block access to a website:

  1. Click the 'Website Restrictions' link under the 'Firewall' menu item.

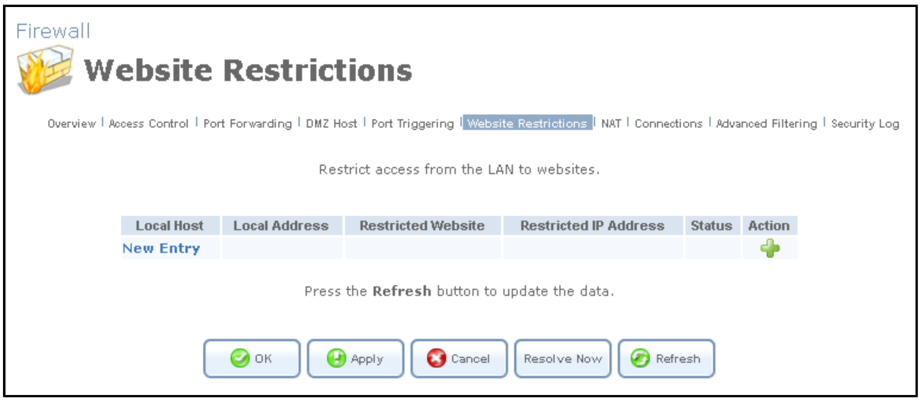


Figure 5.21 Website Restrictions

2. Click the 'New Entry' link. The 'Restricted Website' screen appears.

Figure 5.22 Restricted Website

3. Enter the URL (or part of the URL) that you would like to make inaccessible from your home network (all web pages within this URL will also be blocked). If the URL has multiple IP addresses, OpenRG will resolve all additional addresses and automatically add them to the restrictions table.

4. The 'Local Host' drop-down menu provides you with the ability to specify the computer or group of computers on which you would like to apply the website restriction. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on all OpenRG's LAN hosts. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.

5. By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

6. Click 'OK' to save the settings. You will be returned to the previous screen, while OpenRG attempts to find the site. 'Resolving...' will appear in the 'Status' column while the site is being located (the URL is 'resolved' into one or more IP addresses).

7. Click the 'Refresh' button to update the status if necessary. If the site is successfully located, then 'Resolved' will appear in the status bar. Otherwise, 'Hostname Resolution Failed' will appear. In case OpenRG fails to locate the website, perform the following:

    a. Use a web browser to verify that the website is available. If it is, then you probably entered the website address incorrectly.

    b. If the website is not available, return to the 'Website Restrictions' screen at a later time and click the 'Resolve Now' button to verify that the website can be found and blocked by OpenRG.

You may edit the website restriction by modifying its entry under the 'Local Host' column in the 'Website Restrictions' screen.

- To modify an entry:

    1. Click the action icon for the restriction. The 'Restricted Website' screen appears (see Figure 5.22). Modify the website address, group or schedule as necessary.

    2. Click the 'OK' button to save your changes and return to the 'Website Restrictions' screen.

- To ensure that all current IP addresses corresponding to the restricted websites are blocked, click the 'Resolve Now' button. OpenRG will check each of the restricted website addresses and ensure that all IP addresses at which this website can be found are included in the IP addresses column.

  You can disable a restriction in order to make a website available again without having to remove it from the 'Website Restrictions' screen. This may be useful if you wish to make the website available only temporarily, intending to block it again in the future.

- To temporarily disable a rule, clear the check box next to the service name.

- To reinstate it at a later time, simply reselect the check box.

- To remove a rule, click the service's action icon . The service will be permanently removed.

5.2.6 Using OpenRG's Network Address and Port Translation

OpenRG features a configurable Network Address Translation (NAT) and Network Address Port Translation (NAPT) mechanism, allowing you to control the network addresses and ports set in packets routed through your gateway. When enabling multiple computers on your network to access the Internet using a fixed number of public IP addresses, you can statically define which LAN IP address will be translated to which NAT IP address and/or ports.

By default, OpenRG operates in NAPT routing mode (refer to Section 6.4.7.4.3). However, you can control your network translation by defining static NAT/NAPT rules. Such rules map LAN computers to NAT IP addresses. The NAT/NAPT mechanism is useful for managing Internet usage in your LAN, or complying with various application demands. For example, you can assign your primary LAN computer a single NAT IP address, in order to assure its permanent connection to the Internet. Another example is when an application server to which you would like to connect, such as a security server, requires that packets have a specific IP address—you can define a NAT rule for that address.

5.2.6.1 Configuring the NAT

Click the 'NAT' link under the 'Firewall' menu item. The 'NAT' screen appears.

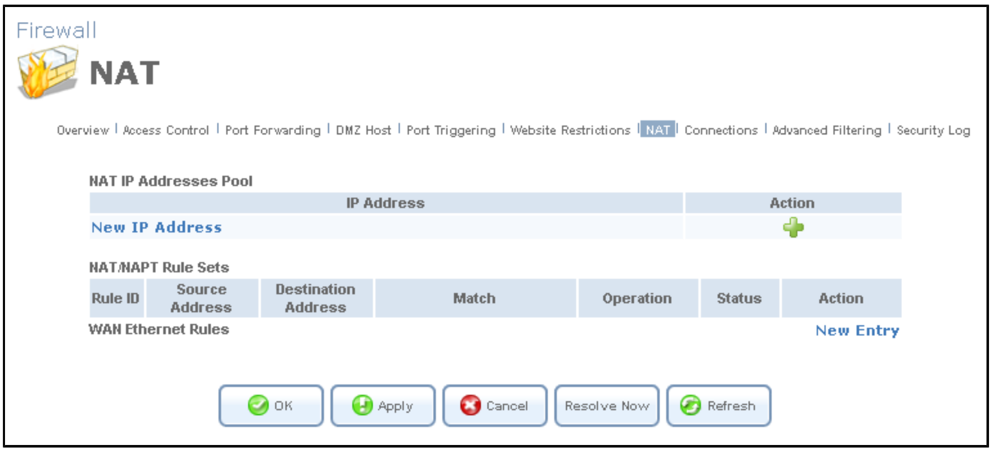


Figure 5.23 Network Address Translation

Before configuring NAT/NAPT rules, you must first enter the additional public IP addresses obtained from your ISP as your NAT IP addresses, in the 'NAT IP Addresses Pool' section.

Note: The primary IP address used by the WAN device for dynamic NAPT should not be added to this table.

To add a NAT IP address, perform the following:

1. Click the 'New IP Address' link. The 'Edit Item' screen appears.

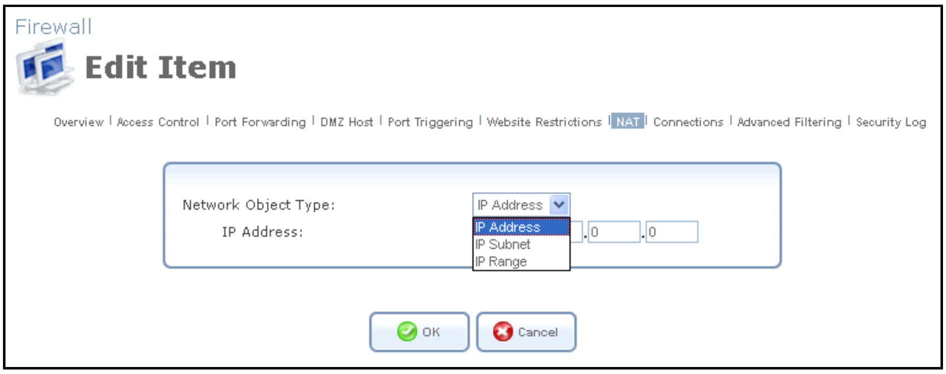


Figure 5.24 Edit Item

2. To add a single public address, select the 'IP Address' option from the 'Network Object Type' drop-down menu, and enter the IP in the fields that appear.

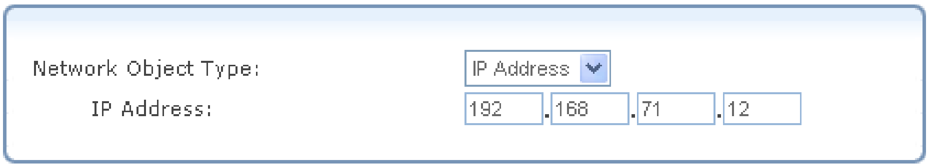


Figure 5.25 Edit Item

To add a range of public IP addresses, select the 'IP Range' option and enter the available IP range.

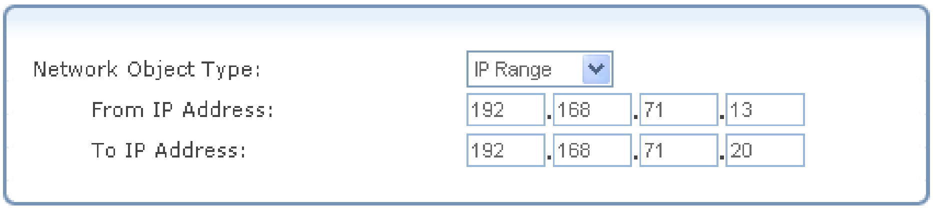


Figure 5.26 Edit Item

3. Click 'OK' to save the settings. The new IP addresses are displayed in the 'NAT IP Addresses Pool' section.

NAT IP Addresses Pool

IP Address	Action
192.168.71.12	
192.168.71.13 - 192.168.71.20	
New IP Address	

Figure 5.27 NAT IP Addresses

To add a new NAT/NAPT rule, click the 'New Entry' link in the 'NAT/NAPT Rule Sets' section of the 'NAT' screen. The 'Add NAT/NAPT Rule' screen appears.

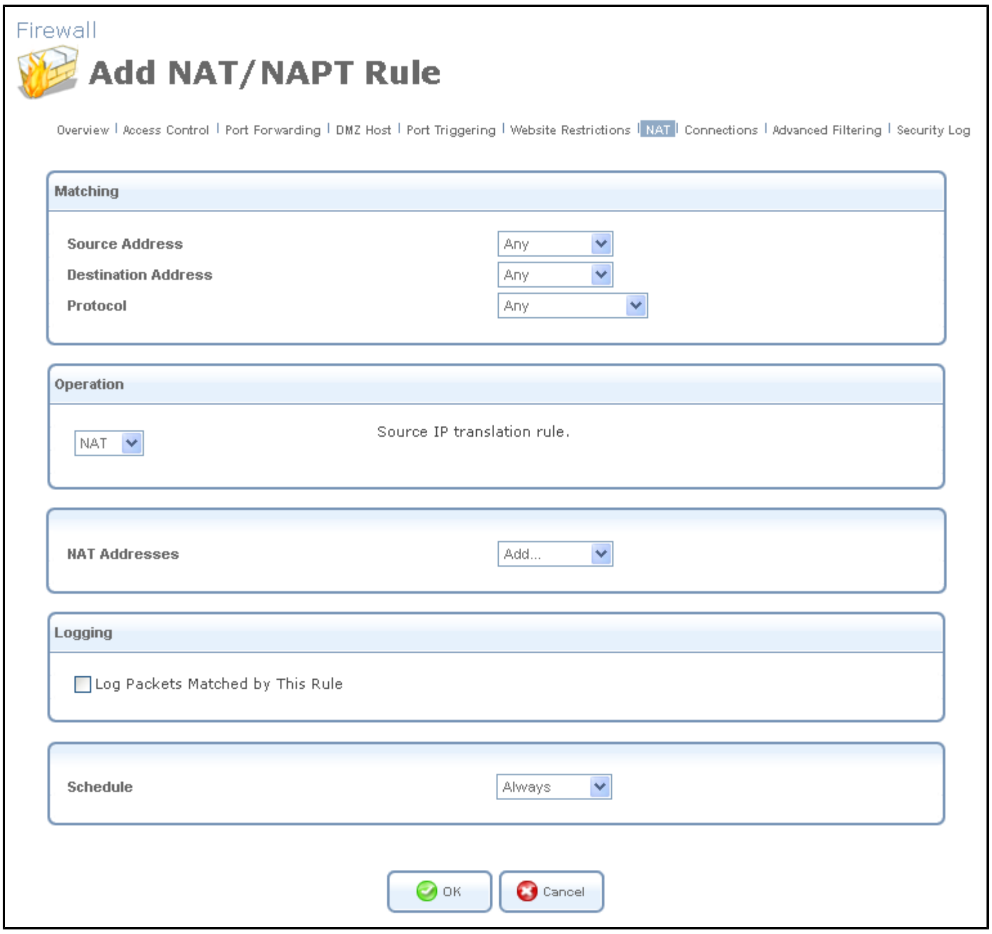


Figure 5.28 Add NAT/NAPT Rule

Matching Use this section to define characteristics of the packets matching the rule.

- **Source Address** The source address of packets sent or received by OpenRG. Use this drop-down menu to specify a LAN computer or a group of LAN computers on which you would like to apply the rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on all OpenRG's LAN hosts. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.

- **Destination Address** The destination address of packets sent or received by OpenRG. This address can be configured in the same manner as the source address. For example, use this drop-down menu to specify an IP address of a remote application server (such as a security server), which requires that the incoming packets have a specific IP address (e.g., one of those defined in your NAT IP address pool).

- **Protocol** You may also specify a traffic protocol. Selecting the 'Show All Services' option from the drop-down menu expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This will commence a sequence that will add a new **Service**, representing the protocol. Refer to Section 6.9.2 in order to learn how to do so.

Operation Use this section to define the operation that will be applied on the IP addresses matching the criteria defined above. The operations available are NAT or NAPT. Selecting each from the drop-down menu refreshes the screen accordingly.

- **NAT Addresses**

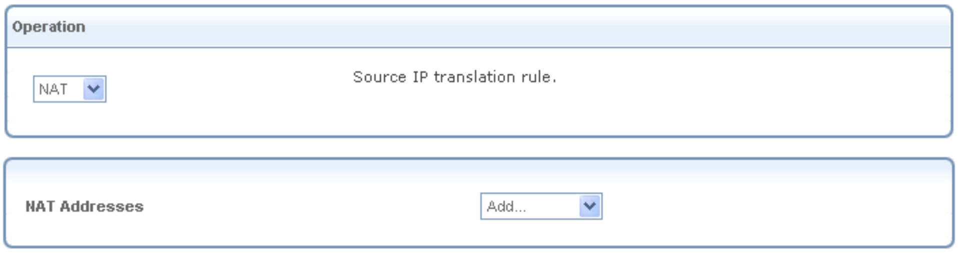


Figure 5.29 Add NAT Rule

This drop-down menu displays all of your available NAT addresses/ranges, from which you can select an entry. If you would like to add a single address or a sub-range from the given pool/range, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.

- **NAPT Address**

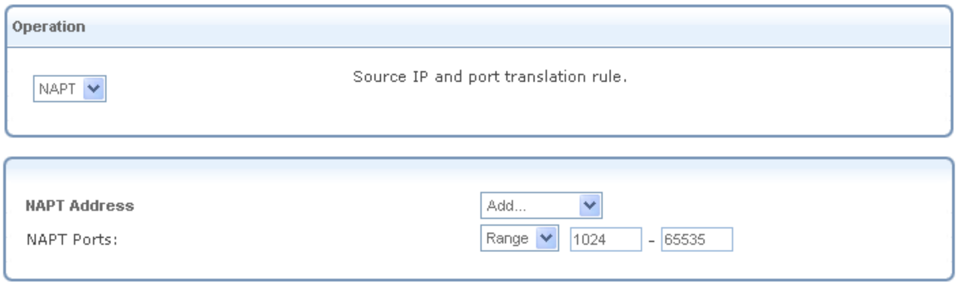


Figure 5.30 Add NAPT Rule

This drop-down menu displays all of your available NAPT addresses/ranges, from which you can select an entry. If you would like to add a single address or a sub-range from the given pool/range, select the 'User Defined' option from the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to Section 6.9.2 in order to learn how to do so. Note, however, that in this case the network object may only be an IP address, as NAPT is port-specific.

- **NAPT Ports** Specify the port(s) for the IP address into which the original IP address will be translated. Enter a single port or select 'Range' in the drop-down menu. The screen refreshes, enabling you to enter a range of ports.

Figure 5.31 Add NAPT Rule

Logging Monitor the rule.

- **Log Packets Matched by This Rule** Select this check box to log the first packet from a connection that was matched by this rule.

Schedule By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

5.2.6.2 NAT/NAPT Configuration Examples

This section demonstrates the NAT/NAPT usage and capabilities, by creating several rules and observing their implementation. In the following examples, the LAN IP address range is 192.168.1.5 through 192.168.1.25. The NAT addresses are 192.168.71.12 through 192.168.71.20, and they have been entered to the NAT address pool as described earlier.

In the 'NAT' screen, click the 'New Entry' link in the 'NAT/NAPT Rule Sets' section. The 'Add NAT/NAPT Rule' screen appears.

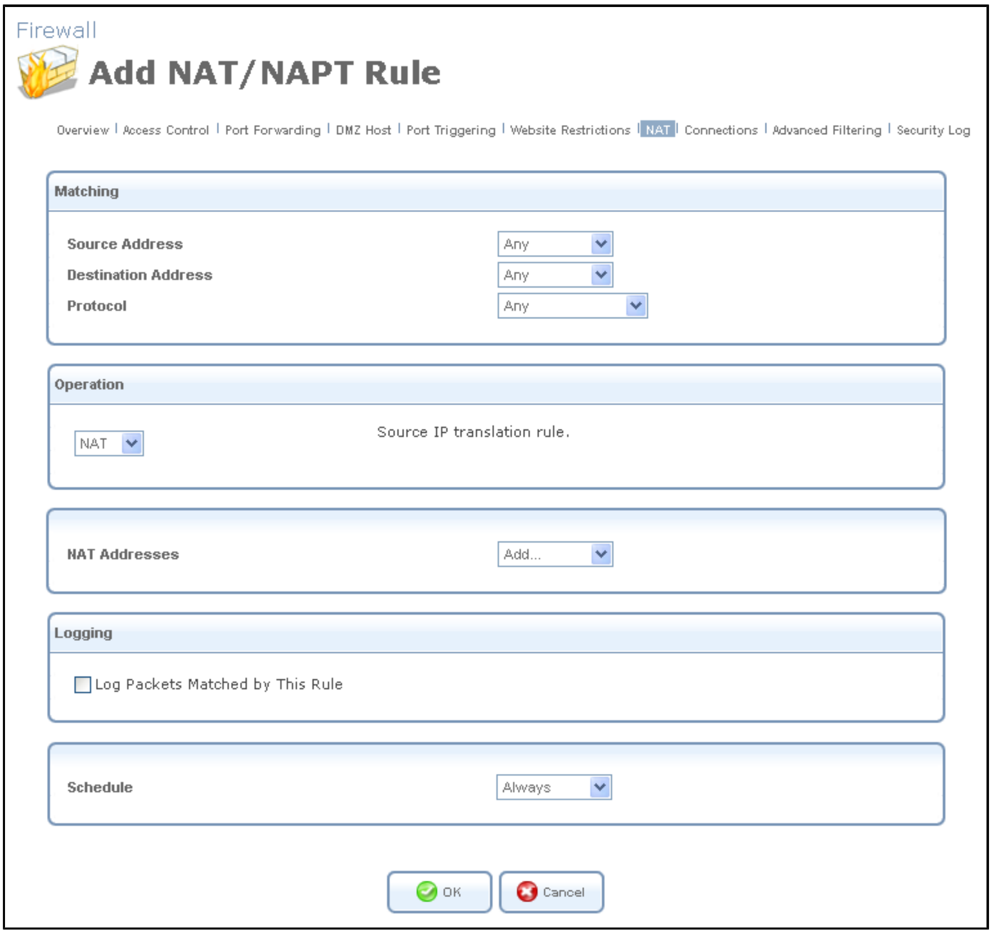


Figure 5.32 Add NAT/NAPT Rule

Create the following NAT/NAPT rules:

1. Translate the address 192.168.1.10 to 192.168.71.12. In this example, LAN addresses (192.168.1.X) are not defined yet, therefore do not appear as drop-down menu options, and network objects must be created in order to represent them.

   a. Select 'User Defined' in the 'Source Address' drop-down menu. The 'Edit Network Object' screen appears.

Figure 5.33 Edit Network Object

   b. Click 'New Entry'. The 'Edit Item' screen appears.

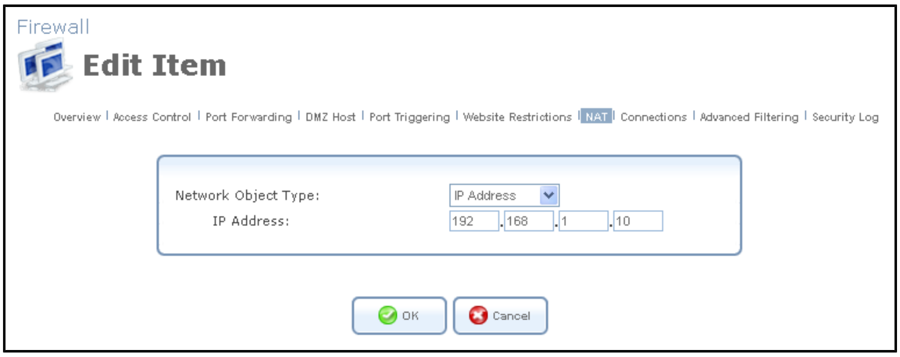


Figure 5.34 Edit Item

   c. Select 'IP Address' in the 'Network Object Type' drop-down menu, and enter 192.168.1.10.

   d. Click 'OK' to save the settings.

   e. Click 'OK' in the 'Edit Network Object' screen.

   f. Back in the 'Add NAT/NAPT Rule' screen, select 192.168.1.10 from the 'Source' drop-down menu.

   g. From the 'NAT Addresses' drop-down menu, select the '192.168.71.12' option. The screen refreshes, adding this address as a NAT IP address.

   h. Click 'OK' to save the settings.

The NAT rule is displayed in the 'NAT' screen.

NAT/NAPT Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
0	192.168.1.10	Any		NAT -> 192.168.71.12	Active	
New Entry						

Figure 5.35 NAT/NAPT Rule Sets

This rule translates one LAN IP address to one NAT IP address, meaning that this LAN computer will have WAN access at any time. The status is therefore set to "Active".

2. Translate the range 192.168.1.11-192.168.1.15 to 192.168.71.12-192.168.71.15. Define this NAT rule in the same manner depicted above, with the exception of selecting 'IP Range' (instead of 'IP Address') as the network object type. Since both ranges are not predefined (no such drop-down menu options), network objects must be created in order to represent them, using the 'User Defined' option in the 'Source' and 'NAT' drop-down menus respectively. The created rule is displayed in the 'NAT' screen.

NAT/NAPT Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
0	192.168.1.10	Any		NAT -> 192.168.71.12	Active	
1	192.168.1.11 - 192.168.1.15	Any		NAT -> 192.168.71.12 - 192.168.71.15	Active	
New Entry						

Figure 5.36 NAT/NAPT Rule Sets

This rule translates five new LAN IP addresses to four NAT IP addresses, which would normally mean that only four of the five LAN computers may have WAN access at the same time. However, note that the NAT address 192.168.71.12 is already in use by the first rule. OpenRG will therefore allow these five LAN computers to use only the three remaining IP addresses ending with 71.13, 71.14 and 71.15. The status is therefore set to "Active".

3. Translate the range 192.168.1.21-192.168.1.25 to 192.168.71.13-192.168.71.14. Define this NAT rule in the same manner depicted above. The following attention message is displayed.

Figure 5.37 Attention

Click 'OK'. The rule is displayed in the 'NAT' screen.

NAT/NAPT Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
0	192.168.1.10	Any		NAT -> 192.168.71.12	Active	
1	192.168.1.11 - 192.168.1.15	Any		NAT -> 192.168.71.12 - 192.168.71.15	Active	
2	192.168.1.21 - 192.168.1.25	Any		NAT -> 192.168.71.13 - 192.168.71.14	Error	
New Entry						

Figure 5.38 NAT/NAPT Rule Sets

This rule translates five new LAN IP addresses to two NAT IP addresses, both of which are already in use by the second rule. OpenRG is therefore unable to resolve this situation and the rule's status is set to "Error". Notice that had this rule been defined as the second rule, all three rules would be valid. This is because the NAT address 192.168.71.15 would still be available for rule number 1. This can easily be amended: you can use the green arrow icons to move a rule entry up or down, changing its priority respectively. Click this rule's action icon once. All rules will now be set to "Active".

NAT/NAPT Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
0	192.168.1.10	Any		NAT -> 192.168.71.12	Active	
2	192.168.1.21 - 192.168.1.25	Any		NAT -> 192.168.71.13 - 192.168.71.14	Active	
1	192.168.1.11 - 192.168.1.15	Any		NAT -> 192.168.71.12 - 192.168.71.15	Active	
New Entry						

Figure 5.39 NAT/NAPT Rule Sets

> Note: The first rule now maps five LAN addresses to one NAT address. OpenRG subtracts all previously used NAT addresses, requested by previous rules, from the requested NAT addresses of the current rule. The requested range of addresses does not determine how many will be available; the number of available addresses is determined by previous rules configuration and order. Rules will appear as "Active" even if they only have one usable NAT address.

4. Translate the address 192.168.1.5 to 192.168.71.16 **ports** 1024-1050. Define this NAPT rule in the same manner depicted above, with the following exception:

   a. Select the 'NAPT' option in the 'Operation' section drop-down menu. The screen refreshes.

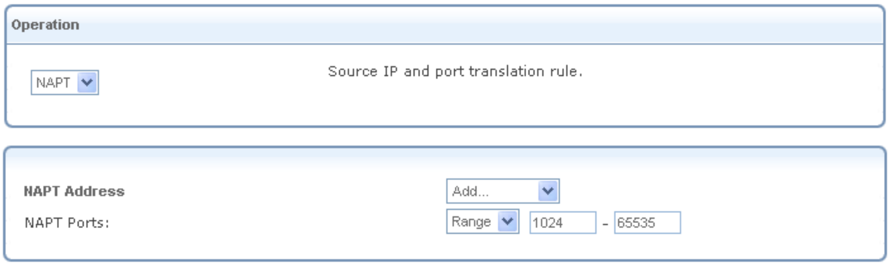


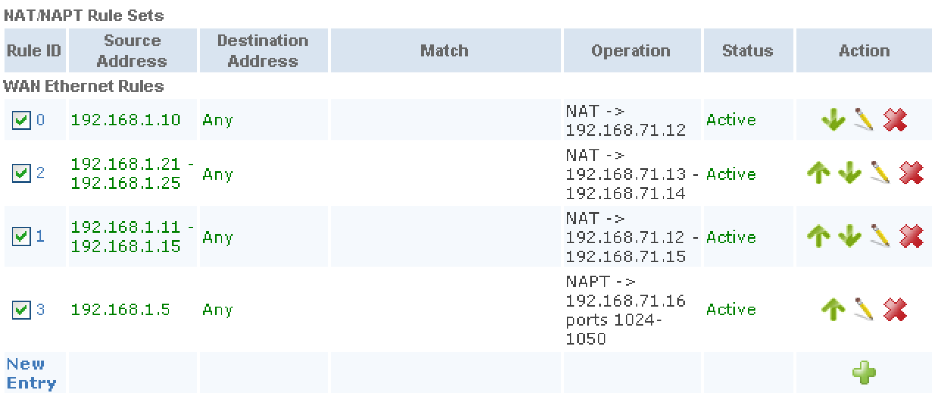
Figure 5.40 Add NAPT Rule

b. Add a NAPT address by selecting the 'User Defined' option.

c. Enter 1024-1050 as the range of ports in the 'NAPT Ports' section.

d. Click 'OK' to save the settings.

The rule is displayed in the 'NAT' screen.



NAT/NAPT Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
0	192.168.1.10	Any		NAT -> 192.168.71.12	Active	
2	192.168.1.21 - 192.168.1.25	Any		NAT -> 192.168.71.13 - 192.168.71.14	Active	
1	192.168.1.11 - 192.168.1.15	Any		NAT -> 192.168.71.12 - 192.168.71.15	Active	
3	192.168.1.5	Any		NAPT -> 192.168.71.16 ports 1024-1050	Active	
New Entry						

Figure 5.41 NAT/NAPT Rule Sets

This rule translates a LAN IP address to a NAT IP address with specific ports. Its status is set to "Active".

5. Translate the address 192.168.1.6 to 192.168.71.16 ports 1024-1100. Define this NAPT rule in the same manner depicted above. The rule is displayed in the 'NAT' screen.

NAT/NAPT Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
0	192.168.1.10	Any		NAT -> 192.168.71.12	Active	
2	192.168.1.21 - 192.168.1.25	Any		NAT -> 192.168.71.13 - 192.168.71.14	Active	
1	192.168.1.11 - 192.168.1.15	Any		NAT -> 192.168.71.12 - 192.168.71.15	Active	
3	192.168.1.5	Any		NAPT -> 192.168.71.16 ports 1024-1050	Active	
4	192.168.1.6	Any		NAPT -> 192.168.71.16 ports 1024-1100	Active	
New Entry						

Figure 5.42 NAT/NAPT Rule Sets

This rule translates a LAN IP address to a NAT IP address with ports 1024-1100. However, only ports 1051-1100 will be used for this LAN computer, as ports 1024-1050 are already in use by the preceding rule. The status is set to "Active".

Every new NAT/NAPT rule is verified in relation to preceding rules. Rules are prioritized according to the order in which they are defined. As long as at least one unused IP address (or port) is available, the rule will be accepted. However, as seen in the examples above, not all addresses in the range defined may be available for computers in that rule; some may already be in use by other rules. OpenRG automatically calculates the relationships between rules, narrowing down the address ranges if needed, and thus provides great flexibility for user input.

The verification performed by OpenRG is as follows:

- NAT rule – Verifies whether the IP address is already in use by another NAT/NAPT rule.
- NAPT rule
  1. Verifies whether the port is already in use by another NAPT rule activated on the same IP address.
  2. Verifies whether the IP address is already in use by another NAT rule.

5.2.7 Configuring the Advanced Filtering Mechanism

Advanced filtering is designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN devices.

To view OpenRG's advanced filtering options, click the 'Advanced Filtering' link of the 'Firewall' menu item. The 'Advanced Filtering' screen appears.

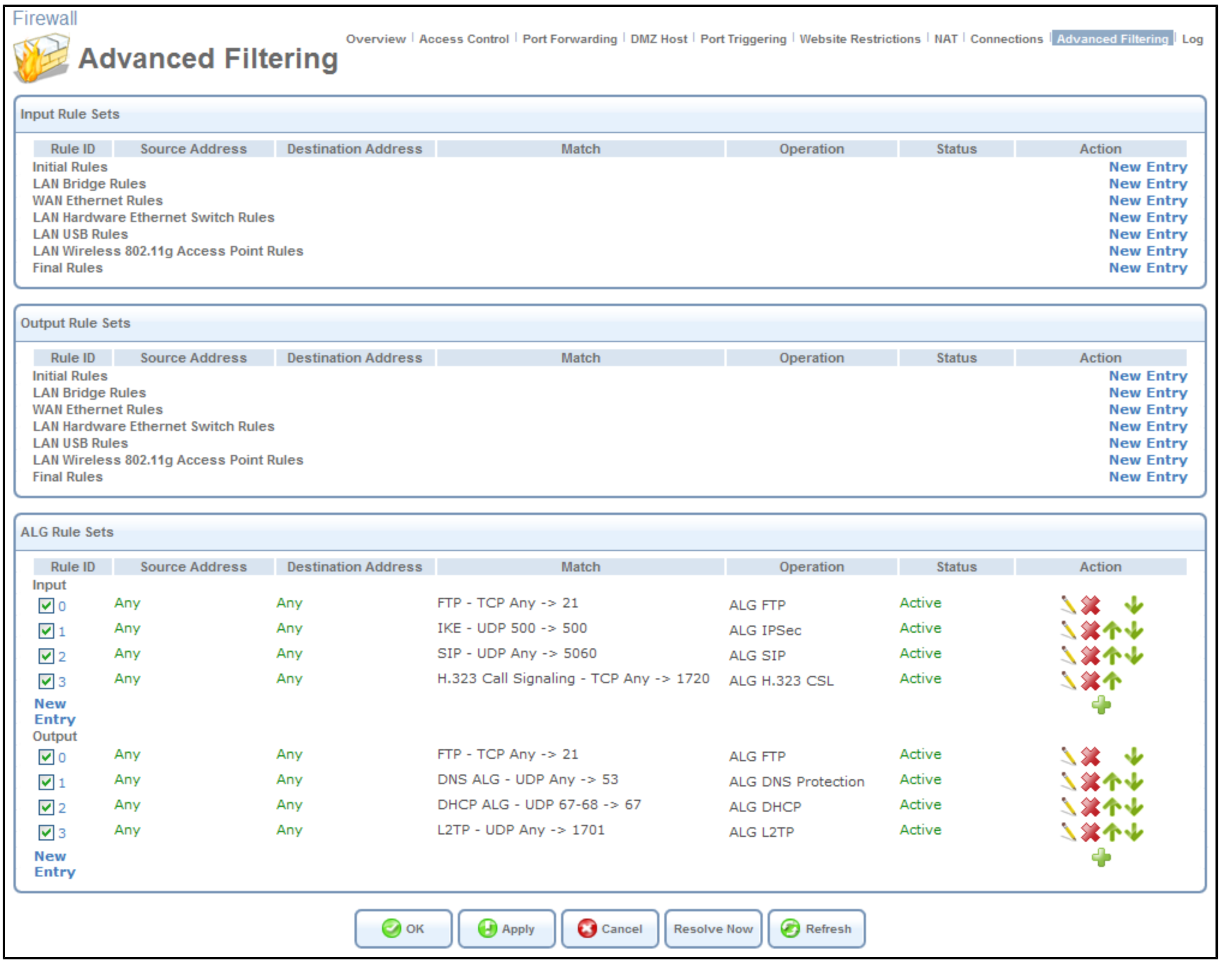


Figure 5.43 Advanced Filtering

5.2.7.1 Adding Input and Output Rules

The first two sections of the 'Advanced Filtering' screen—'Input Rule Sets' and 'Output Rule Sets', are designed for configuring inbound and outbound traffic respectively. Each section is comprised of subsets, which can be grouped into three main subjects:

- Initial rules – rules defined here will be applied first, on all gateway devices.
- Network devices rules – rules can be defined per each gateway device.
- Final rules – rules defined here will be applied last, on all gateway devices.

There are numerous rules that are automatically created by the firewall in order to provide improved security and block harmful attacks.

To add an advanced filtering rule, first choose the traffic direction and the device on which to set the rule. Then click the appropriate 'New Entry' link. The 'Add Advanced Filter' screen appears.

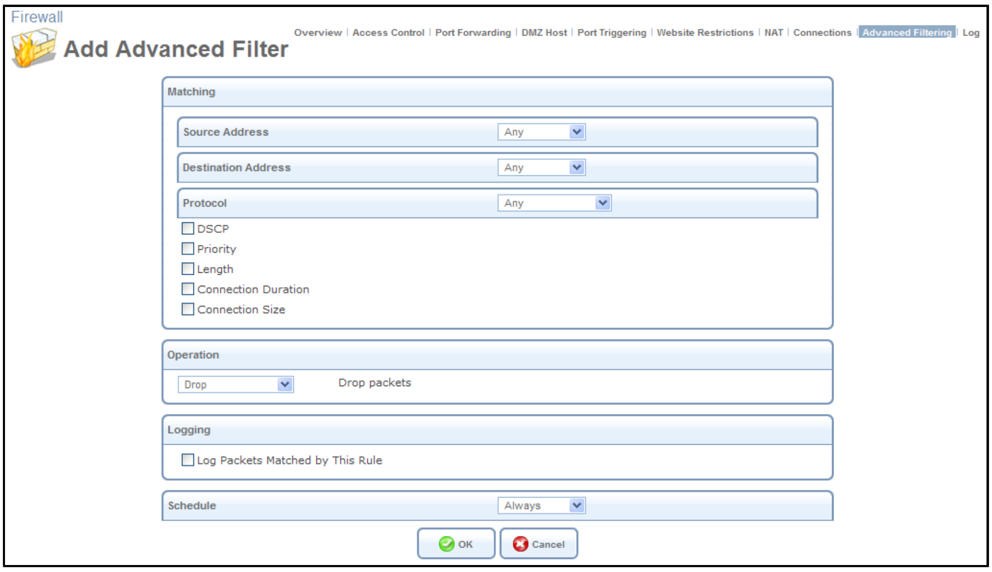


Figure 5.44 Add Advanced Filter

The 'Matching' and 'Operation' sections of this screen define the operation to be executed when matching conditions apply.

Matching Use this section to define characteristics of the packets matching the rule.

- **Source Address** The source address of packets sent or received by OpenRG. Use this drop-down menu to specify the computer or group of computers on which you would like to apply the rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on any host trying to send data. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.

- **Destination Address** The destination address of packets sent or received by OpenRG. This address can be configured in the same manner as the source address. For example, use this drop-down menu to specify an IP address of a remote application server (such as a security server), which requires that the incoming packets have a specific IP address (e.g., one of those defined in your NAT IP address pool).

- **Protocol** You may also specify a traffic protocol. Selecting the 'Show All Services' option from the drop-down menu expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This will commence a sequence that will add a new **Service**, representing the protocol. Refer to Section 6.9.2 in order to learn how to do so.

- **DSCP** Select this check box to display two DSCP fields, which enable you to specify a hexadecimal DSCP value and its mask assigned to the packets matching the priority rule. For more information, refer to Section 5.3.5.

- **Priority** Select this check box to display a drop-down menu, in which you can select a priority level assigned to the packets matching the priority rule. For more information, refer to Section 5.3.3.

- **Length** Select this check box if you would like to specify the length of packets, or the length of their data portion.

> Note: The following two options are applicable only if the Fastpath feature is disabled in the 'Routing' menu item under 'System'. Depending on your gateway's model, the feature's name may appear as 'Software Acceleration' or 'Hardware Acceleration'.

- **Connection Duration** Select this check box to apply the priority rule only on connections which are open for a certain time period. This option is especially useful if you would like to accelerate your Web browsing by lowering the speed of concurrently running download jobs, or vice versa. After selecting the check box, choose whether the duration of connections matching the rule should be greater or less than the time that you specify in the adjacent field.

Figure 5.45 Connection Duration

For example, if you define the connection duration as less than 10 seconds, you will notice acceleration of your Web browsing and small file downloads, but slowing down of your large file downloads. The reason for this is that when a connection passes the specified time limit (as in case of a large file download), its priority is lowered, thereby giving more priority to shorter connections.

- **Connection Size** Select this check box to apply the priority rule only on connections matching a certain data size limit. This option is best used along with the 'Connection Duration' option, enabling you to fine-tune the gateway's traffic priority mechanism according to your needs. After selecting the check box, choose whether the connection's data size should be greater or less than the number of kilobytes that you specify in the adjacent field.

Figure 5.46 Connection Size

For example, if you define the connection size as less than 400 kilobytes, you will notice acceleration of Web browsing, and lowering of your file download speed. The reason for this is that when a connection exceeds the specified data size limit, its priority is lowered, thereby giving more priority to connections with a smaller data size.

Operation Define what action the rule will take, by selecting one of the following radio buttons:

- **Drop** Deny access to packets that match the source and destination IP addresses and service ports defined above.

- **Reject** Deny access to packets that match the criteria defined, and send an ICMP error or a TCP reset to the origination peer.

- **Accept Connection** Allow access to packets that match the criteria defined. The data transfer session will be handled using Stateful Packet Inspection (SPI), meaning that other packets matching this rule will be automatically allowed access.

- **Accept Packet** Allow access to packets that match the criteria defined. The data transfer session will not be handled using SPI, meaning that other packets matching this rule will not be automatically allowed access. This can be useful, for example, when creating rules that allow broadcasting.

Logging Monitor the rule.

- **Log Packets Matched by This Rule** Select this check box to log the first packet from a connection that was matched by this rule.

Schedule By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

The order of the rules' appearance represents both the order in which they were defined and the sequence by which they will be applied. You may change this order after your rules are already defined (without having to delete and then re-add them), by using the action icon and action icon .

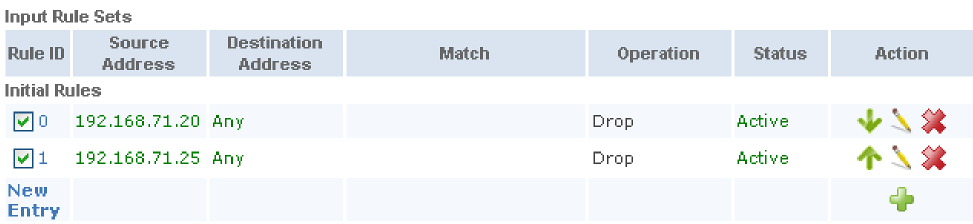


Figure 5.47 Move Up and Move Down Action Icons

5.2.7.2 Adding ALG Rules

The 'ALG Rule Sets' section enables you to define address and port processing rules for certain application protocols (such as, FTP, TFTP, SIP, and others), which carry the IP address inside the application data. Most of these protocols will not work with the NAT, unless the NAT is aware of them and does the appropriate translation.

The NAT is application independent, therefore a specific Application Level Gateway (ALG) is required to perform payload monitoring and needed alterations to allow the application's traffic to pass through the firewall. The 'Input' and 'Output' subsections of the 'ALG Rule Sets' feature (see Figure 5.43) are designated to display ALG rules for inbound and outbound traffic respectively. Note that OpenRG is automatically configured with ALG rules for several widespread protocols. You can edit a rule by clicking its respective action icon , or remove it by clicking the action icon .

To create an ALG rule, either inbound or outbound, click the 'New Entry' link that corresponds to the rule type you would like to define. The 'Add ALG Rule' screen appears.

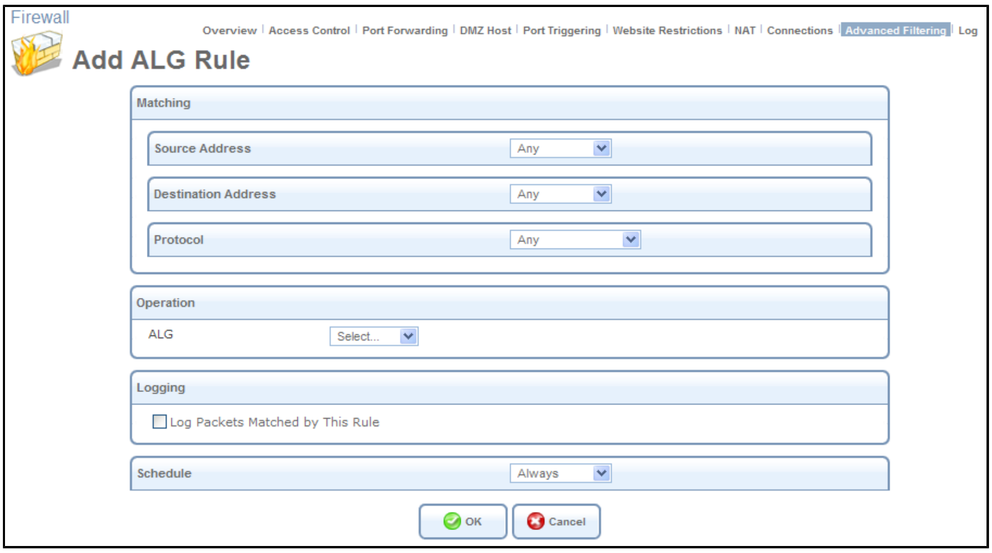


Figure 5.48 Add ALG Rule

The 'Matching' and 'Operation' sections of this screen define the operation to be executed when matching conditions apply.

Matching Use this section to define characteristics of the packets matching the rule.

- **Source Address** The source address of packets sent or received by OpenRG. Use this drop-down menu to specify the computer or group of computers on which you would like to apply the rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on any host trying to send data. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.

- **Destination Address** The destination address of packets sent or received by OpenRG. This address can be configured in the same manner as the source address. For example, use this drop-down menu to specify an IP address of a remote application server (such as a security server), which requires that the incoming packets have a specific IP address (e.g., one of those defined in your NAT IP address pool).

- **Protocol** You may also specify a traffic protocol. Selecting the 'Show All Services' option from the drop-down menu expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This will commence a sequence that will add a new **Service**, representing the protocol. Refer to Section 6.9.2 in order to learn how to do so.

Operation Define which ALG will be used, by selecting one from the designated drop-down menu.

Logging Monitor the rule.

- **Log Packets Matched by This Rule** Select this check box to log the first packet from a connection that was matched by this rule.

Schedule By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

> Note: The defined ALG rule will also be applied to the child processes of the application that utilizes the selected protocol.

The order of the rules' appearance represents both the order in which they were defined and the sequence by which they will be applied. You may change this order after your rules are already defined (without having to delete and then re-add them), by using the action icon and action icon .

5.2.8 Viewing the Firewall Log

The 'Firewall Log' screen displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate through an administrative interface (WBM or Telnet terminal), firewall configuration and system start-up.

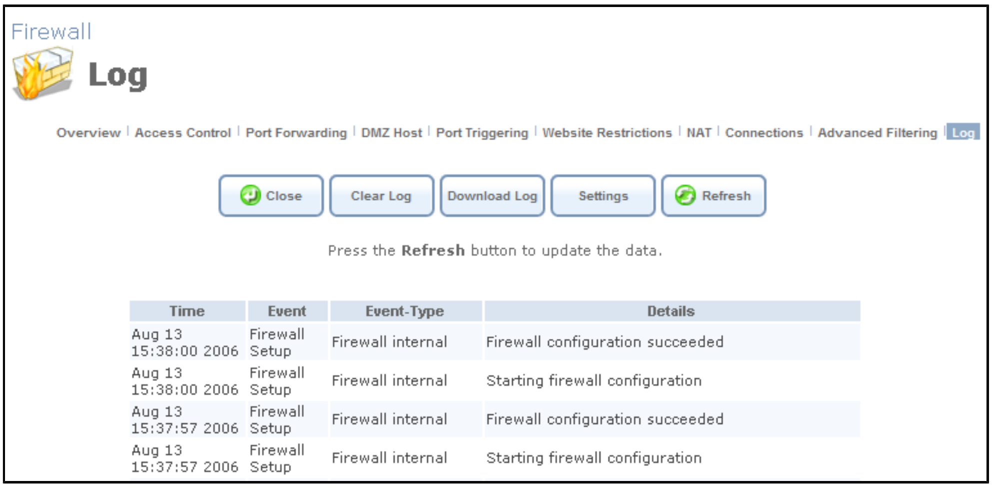


Figure 5.49 Firewall Log

The log's columns are:

Time The time the event occurred.

Event There are five kinds of events:

- Inbound Traffic: The event is a result of an incoming packet.
- Outbound Traffic: The event is a result of outgoing packet.
- Firewall Setup: Configuration message.
- WBM Login: Indicates that a user has logged in to WBM.
- CLI Login: Indicates that a user has logged in to CLI (via Telnet).

Event-Type A textual description of the event:

- Blocked: The packet was blocked. The message is colored red.
- Accepted: The packet was accepted. The message is colored green.

Details More details about the packet or the event, such as protocol, IP addresses, ports, etc.
Use the buttons at the top of the page to:

Close Close the 'Log' screen and return to OpenRG's home page.

Clear Log Clear all currently displayed log messages.

Download Log Download the log as a Comma Separated Value (CSV) file, named **firewall.csv**.

Settings View or change the security log settings (explanation follows).

Refresh Refresh the screen to display the latest updated log messages.

To view or change the security log settings:

1. Click the 'Settings' button that appears at the top of the 'Firewall Log' screen. The 'Log Settings' screen appears.

Figure 5.50 Log Settings

2. Select the types of activities for which you would like to have a log message generated:

    - Accepted Events

      Accepted Incoming Connections Write a log message for each successful attempt to establish an inbound connection to the home network.

      Accepted Outgoing Connections Write a log message for each successful attempt to establish an outgoing connection to the public network.

    - Blocked Events

      All Blocked Connection Attempts Write a log message for each blocked attempt to establish an inbound connection to the home network or vice versa. You can enable logging of blocked packets of specific types by disabling this option, and enabling some of the more specific options below it.

      Specific Events Specify the blocked events that should be monitored. Use this to monitor specific event such as SynFlood. A log message will be generated if either the corresponding check box is selected, or the "All Blocked Connection Attempts" check box is selected.

    - Other Events

      Remote Administration Attempts Write a log message for each remote administration connection attempt, whether successful or not.

      Connection States Provide extra information about every change in a connection opened by the firewall. Use this option to track connection handling by the firewall and Application Level Gateways (ALGs).

    - Log Buffer

      Prevent Log Overrun Select this check box in order to stop logging firewall activities when the memory allocated for the log fills up.

3. Click 'OK' to save the settings.

5.2.8.1 The Firewall Event Types

The following are the available event types that can be recorded in the firewall log:

1. Firewall internal – an accompanying explanation from the firewall internal mechanism will be added in case this event–type is recorded.

2. Firewall status changed – the firewall changed status from up to down or the other way around, as specified in the event type description.

3. STP packet – an STP packet has been accepted/rejected.

4. Illegal packet options – the options field in the packet's header is either illegal or forbidden.
5. Fragmented packet – a fragment has been rejected.
6. WinNuke protection – a WinNuke attack has been blocked.
7. ICMP replay – an ICMP replay message has been blocked.
8. ICMP redirect protection – an ICMP redirected message has been blocked.
9. Packet invalid in connection – a packet has been blocked, being on an invalid connection.
10. ICMP protection – a broadcast ICMP message has been blocked.
11. Broadcast/Multicast protection – a packet with a broadcast/multicast source IP has been blocked.
12. Spoofing protection – a packet from the WAN with a source IP of the LAN has been blocked.
13. DMZ network packet – a packet from a demilitarized zone network has been blocked.
14. Trusted device – a packet from a trusted device has been accepted.
15. Default policy – a packet has been accepted/blocked according to the default policy.
16. Remote administration – a packet designated for OpenRG management has been accepted/blocked.
17. Access control – a packet has been accepted/blocked according to an access control rule.
18. Parental control – a packet has been blocked according to a parental control rule.
19. NAT out failed – NAT failed for this packet.
20. DHCP request – OpenRG sent a DHCP request (depends on the distribution).
21. DHCP response – OpenRG received a DHCP response (depends on the distribution).
22. DHCP relay agent – a DHCP relay packet has been received (depends on the distribution).
23. IGMP packet – an IGMP packet has been accepted.
24. Multicast IGMP connection – a multicast packet has been accepted.
25. RIP packet – a RIP packet has been accepted.
26. PPTP connection – a packet inquiring whether OpenRG is ready to receive a PPTP connection has been accepted.

27. Kerberos key management 1293 – security related, for future use.
28. Kerberos 88 – for future use.
29. AUTH:113 request – an outbound packet for AUTH protocol has been accepted (for maximum security level).
30. Packet-Cable – for future use.
31. IPV6 over IPV4 – an IPv6 over IPv4 packet has been accepted.
32. ARP – an ARP packet has been accepted.
33. PPP Discover – a PPP discover packet has been accepted.
34. PPP Session – a PPP session packet has been accepted.
35. 802.1Q – a 802.1Q (VLAN) packet has been accepted.
36. Outbound Auth1X – an outbound Auth1X packet has been accepted.
37. IP Version 6 – an IPv6 packet has been accepted.
38. OpenRG initiated traffic – all traffic that OpenRG initiates is recorded.
39. Maximum security enabled service – a packet has been accepted because it belongs to a permitted service in the maximum security level.
40. SynCookies Protection – a SynCookies packet has been blocked.
41. ICMP Flood Protection – a packet has been blocked, stopping an ICMP flood.
42. UDP Flood Protection – a packet has been blocked, stopping a UDP flood.
43. Service – a packet has been accepted because of a certain service, as specified in the event type.
44. Advanced Filter Rule – a packet has been accepted/blocked because of an advanced filter rule.
45. Fragmented packet, header too small – a packet has been blocked because after the defragmentation, the header was too small.
46. Fragmented packet, header too big – a packet has been blocked because after the defragmentation, the header was too big.
47. Fragmented packet, drop all – not used.
48. Fragmented packet, bad align – a packet has been blocked because after the defragmentation, the packet was badly aligned.

49. Fragmented packet, packet too big – a packet has been blocked because after the defragmentation, the packet was too big.

50. Fragmented packet, packet exceeds – a packet has been blocked because defragmentation found more fragments than allowed.

51. Fragmented packet, no memory – a fragmented packet has been blocked because there was no memory for fragments.

52. Fragmented packet, overlapped – a packet has been blocked because after the defragmentation, there were overlapping fragments.

53. Defragmentation failed – the fragment has been stored in memory and blocked until all fragments arrived and defragmentation could be performed.

54. Connection opened – usually a debug message regarding a connection.

55. Wildcard connection opened – usually a debug message regarding a connection.

56. Wildcard connection hooked – usually debug message regarding connection.

57. Connection closed – usually a debug message regarding a connection.

58. Echo/Chargen/Quote/Snork protection – a packet has been blocked, protecting from Echo/Chargen/Quote/Snork.

59. First packet in connection is not a SYN packet – a packet has been blocked because of a TCP connection that had started without a SYN packet.

60. Error: No memory – a message notifying that a new connection has not been established because of lack of memory.

61. NAT Error: Connection pool is full – a message notifying that a connection has not been created because the connection pool is full.

62. NAT Error: No free NAT IP – a message notifying that there is no free NAT IP, therefore NAT has failed.

63. NAT Error: Conflict Mapping already exists – a message notifying that there is a conflict since the NAT mapping already exists, therefore NAT has failed.

64. Malformed packet: Failed parsing – a packet has been blocked because it is malformed.

65. Passive attack on ftp-server: Client attempted to open Server ports – a packet has been blocked because of an unauthorized attempt to open a server port.

66. FTP port request to 3rd party is forbidden (Possible bounce attack) – a packet has been blocked because of an unauthorized FTP port request.

67. Firewall Rules were changed – the firewall rule set has been modified.

68. User authentication – a message during login time, including both successful and failed authentication.

69. First packet is Invalid – first packet in connection failed to pass firewall or NAT.

5.3 Managing Your Bandwidth with Quality of Service

Network-based applications and traffic are growing at a high rate, producing an ever-increasing demand for bandwidth and network capacity. For obvious reasons, bandwidth and capacity cannot be expanded infinitely, requiring that bandwidth-demanding services be delivered over existing infrastructure, without incurring additional, expansive investments.

The next logical means of ensuring optimal use of existing resources are Quality of Service (QoS) mechanisms for congestion management and avoidance. Quality of Service refers to the capability of a network device to provide better service to selected network traffic. This is achieved by shaping the traffic and processing higher priority traffic before lower priority traffic.

As Quality of Service is dependent on the "weakest link in the chain", failure of but a single component along the data path to assure priority packet transmission can easily cause a VoIP call or a Video on Demand (VoD) broadcast to fail miserably. QoS must therefore obviously be addressed end-to-end.

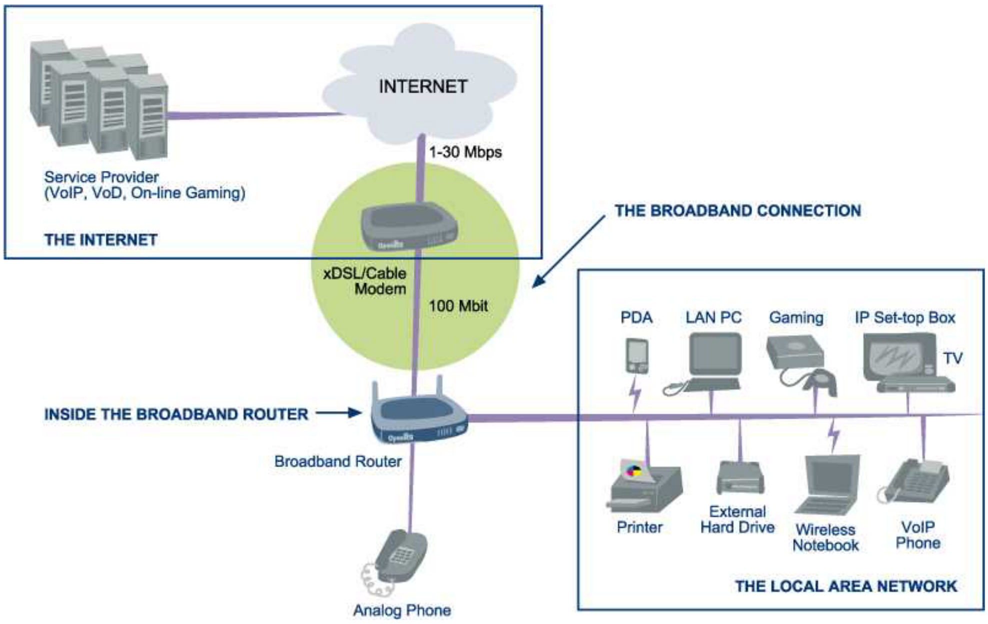


Figure 5.51 End-to-end QoS Challenge Areas

The following are the potential bottleneck areas that need be taken into consideration when implementing an end-to-end QoS-enabled service.

- **The Local Area Network** LANs have finite bandwidth, and are typically limited to 100 Mbps. When given the chance, some applications will consume all available network

bandwidth. In business networks, a large number of network-attached devices can lead to congestion. The need for QoS mechanisms is more apparent in wireless LANs (802.11a/b/g), where bandwidth is even more limited (typically no more than 20 Mbps on 802.11g networks).

- **The Broadband Router** All network traffic passes through and is processed by the broadband router. It is therefore a natural focal point for QoS implementation. Lack of sufficient buffer space, memory or processing power, and poor integration among system components can result in highly undesirable real-time service performance. The only way to assure high quality of service is the use of proper and tightly-integrated router operating system software and applications, which can most effectively handle multiple real-time services simultaneously.

- **The Broadband Connection** Typically the most significant bottleneck of the network, this is where the high speed LAN meets limited broadband bandwidth. Special QoS mechanisms must be built into routers to ensure that this sudden drop in connectivity speed is taken into account when prioritizing and transmitting real-time service-related data packets.

- **The Internet** Internet routers typically have a limited amount of memory and bandwidth available to them, so that congestions may easily occur when links are over-utilized, and routers attempt to queue packets and schedule them for retransmission. One must also consider the fact that while Internet backbone routers take some prioritization into account when making routing decisions, all data packets are treated equally under congested conditions.

The following figure depicts OpenRG's QoS role and architecture in a network. Many of the terms it contains will become familiar as you read on.

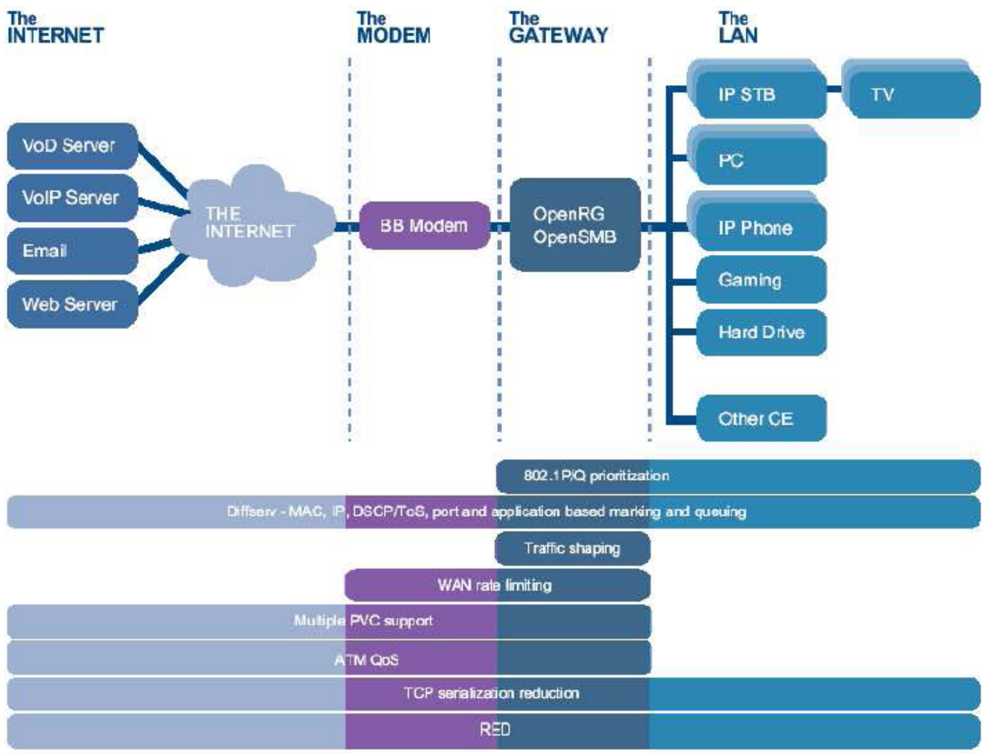


Figure 5.52 OpenRG's QoS Architecture

5.3.1 Selecting a QoS Profile

The 'General' screen provides a Quality of Service "wizard", with which you can configure your QoS parameters according to predefined profiles, with just a few clicks. A chosen QoS profile will automatically define QoS rules, which you can view and edit in the rest of the QoS tab screens, described later.

> Note: Selecting a QoS profile will cause all previous QoS configuration settings to be **permanently lost**.

Click the QoS tab under 'Services'. The 'General' screen appears with the 'Overview' link being selected.

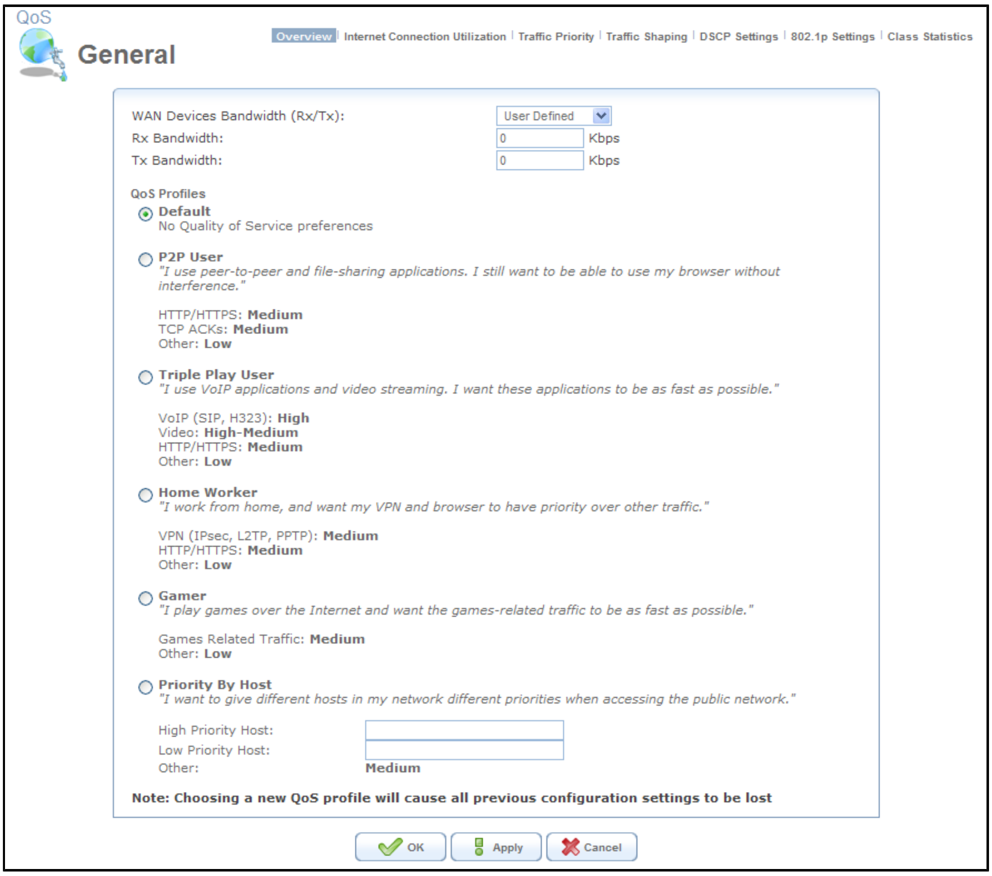


Figure 5.53 General

WAN Devices Bandwidth (Rx/Tx) Before selecting the QoS profile that mostly suits your needs, select your bandwidth from this drop-down menu. If you do not see an appropriate entry, select 'User Defined', and enter your Tx and Rx bandwidths manually.

- **Tx Bandwidth** This parameter defines the gateway's outbound transmission rate. Enter your Tx bandwidth in Kbits per second.
- **Rx Bandwidth** This parameter defines the gateway's Internet traffic reception rate. Enter your Rx bandwidth in Kbits per second.

> Note: By default, these parameters are set to 0 Kbps, which means that the bandwidth has not been limited on OpenRG. Entering inaccurate Tx/Rx values will cause incorrect behavior of the QoS module. It is important to set these values as accurately as possible.

If you wish to restore the default bandwidth settings, select 'Unlimited' from the drop-down menu, and click 'Apply'. Note that you can also set the desired bandwidth on the WAN (or any other) device in the 'Traffic Shaping' screen (to learn how to do so, refer to Section 5.3.4.1).

QoS Profiles Select the profile that mostly suits your bandwidth usage. Each profile entry displays a quote describing what the profile is best used for, and the QoS priority levels granted to each bandwidth consumer in this profile.

- Default – No QoS profile, however the device is limited by the requested bandwidth, if specified.
- P2P User – Peer-to-peer and file sharing applications will receive priority.
- Triple Play User – VoIP and video streaming will receive priority.
- Home Worker – VPN and browsing will receive priority.
- Gamer – Game-related traffic will receive priority.
- Priority By Host – This entry provides the option to configure which computer in your LAN will receive the highest priority and which the lowest. If you have additional computers, they will receive medium priority.

  High Priority Host Enter the host name or IP address of the computer to which you would like to grant the highest bandwidth priority.

  Low Priority Host Enter the host name or IP address of the computer to which you would like to grant the lowest bandwidth priority.

5.3.2 Viewing Your Bandwidth Utilization

The 'Internet Connection Utilization' screen provides detailed real-time information regarding the usage of your Internet connection's bandwidth. At any time, you can view an up-to-date bandwidth usage report on both the application and computer level.

5.3.2.1 Application View

The 'Utilization by Application' table displays the following information fields. You can sort the table according to these fields (ascending or descending), by clicking the fields' names. Note that you can stop the screen's refreshing by using the 'Automatic Refresh Off' button at the bottom of the screen.

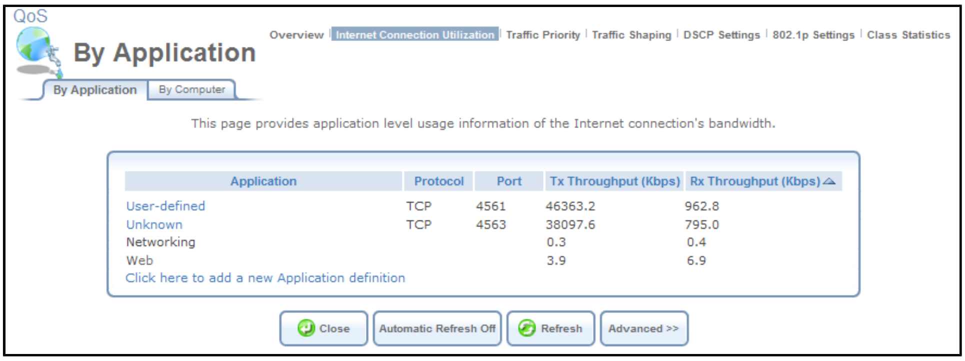


Figure 5.54 Utilization by Application

Application A list of categories of applications that are currently using the bandwidth. This section may also display user-defined or unknown applications that had not been identified by OpenRG as belonging to one of the pre-defined categories. In this case, their names will appear as links, which you can click to view their details.

Protocol The application's network protocol.

Port The port through which traffic is transferred.

Tx Throughput The transmission bit rate in kilo-bits per second.

Rx Throughput The reception bit rate in kilo-bits per second.

OpenRG does not recognize all possible applications running on LAN computers, and marks such an application as "Unknown". You can define an unknown application by clicking the 'Click Here to Add a New Application Definition' link at the bottom of the table. The 'Protocols' screen appears, in which you can define the application by adding it as a new service entry. To learn more about adding protocols, refer to Section 6.9.1.

To view the applications that underlie the displayed categories, click the 'Advanced' button.

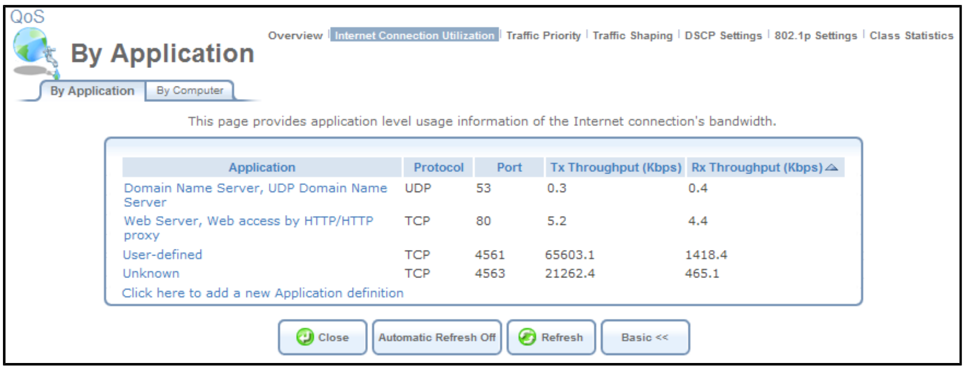


Figure 5.55 Utilization by Application – Advanced View

In this view, you can click each application's name to view its details, particularly which LAN computer is running it.

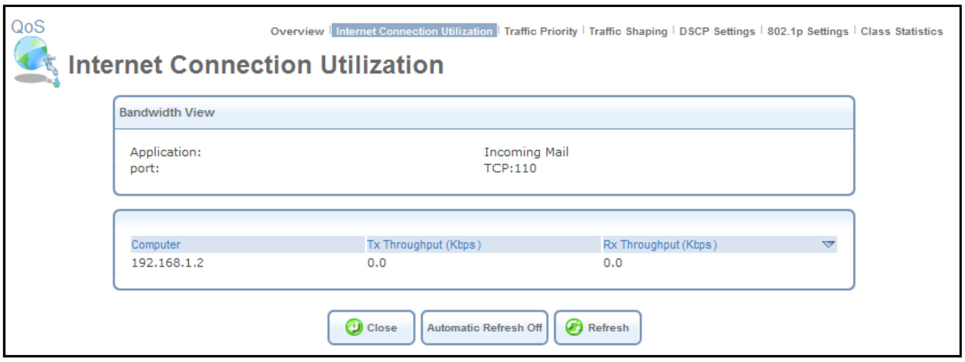


Figure 5.56 A Specific Application

5.3.2.2 Computer View

The 'Utilization by Computer' table displays the sum of bandwidth used by each LAN computer. The fields displayed are the computer's IP address and the Tx and Rx throughput.

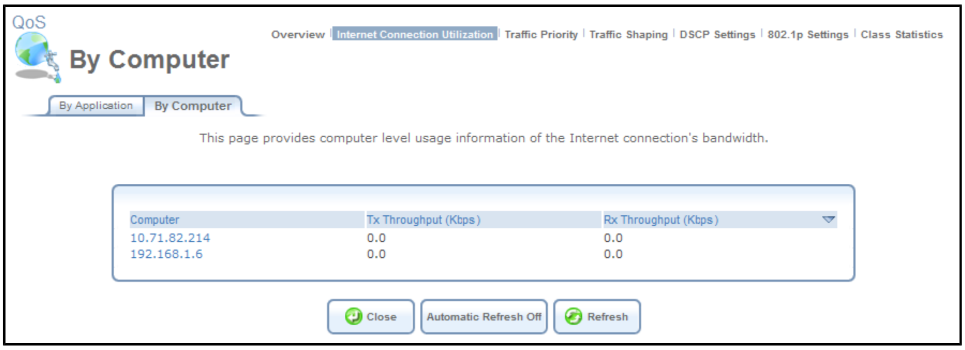


Figure 5.57 Utilization by Computer

Click a computer's IP address to view the bandwidth-consuming applications running on that computer.

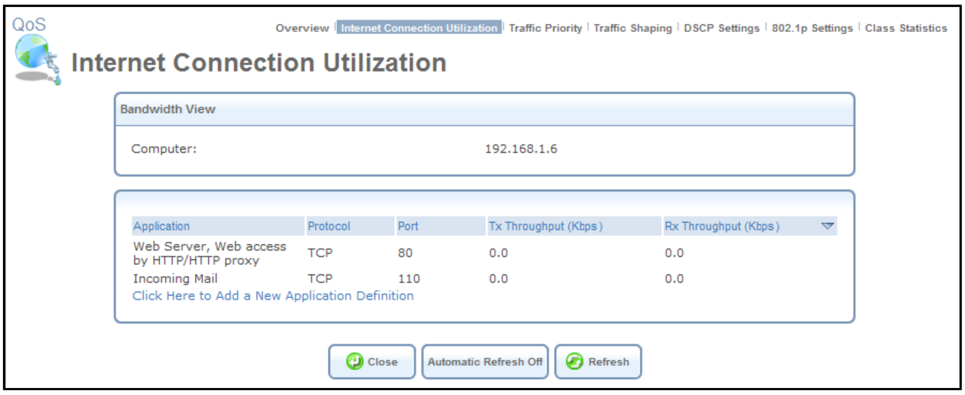


Figure 5.58 A Specific Computer

In this example, computer 192.168.1.6 is running the applications "Web Server" and "Incoming Mail". This screen provides a combined computer and application view, by displaying a computer-specific application table.

5.3.3 Defining Traffic Priority Rules

Traffic Priority allows you to manage and avoid traffic congestion by defining inbound and outbound priority rules for each device on your gateway. These rules determine the priority that packets, traveling through the device, will receive. QoS parameters (DSCP marking and packet priority) are set per packet, on an application basis. You can set QoS parameters using flexible rules, according to the following parameters:

- Source/destination IP address, MAC address or host name
- Device
- Source/destination ports
- Limit the rule for specific days and hours

OpenRG supports two priority marking methods for packet prioritization:

- DSCP (refer to Section 5.3.5).
- 802.1p Priority (refer to Section 5.3.6).

The matching of packets by rules is connection-based, known as Stateful Packet Inspection (SPI), using the same connection-tracking mechanism used by OpenRG's firewall. Once a packet matches a rule, all subsequent packets with the same attributes receive the same QoS parameters, both inbound and outbound. A packet can match more than one rule. Therefore:

- The first class rule has precedence over all other class rules (scanning is stopped once the first rule is reached).
- The first traffic-priority (classless) rule has precedence over all other traffic-priority rules.
- There is no prevention of a traffic-priority rule conflicting with a class rule. In this case, the priority and DSCP setting of the class rule (if given) will take precedence.

Connection-based QoS also allows inheriting QoS parameters by some of the applications that open subsequent connections. For instance, you can define QoS rules on SIP, and the rules will apply to both control and data ports (even if the data ports are unknown). This feature applies to all applications that have ALG in the firewall, such as:

- SIP
- MSN Messenger/Windows Messenger
- TFTP
- FTP
- MGCP

- H.323
- Port Triggering applications (refer to Section 5.2.4)
- PPTP
- IPSec

To set traffic priority rules:

1. Under the 'QoS' menu item, click 'Traffic Priority'. The 'Traffic Priority' screen appears (see Figure 5.59). This screen is divided into two identical sections, one for 'QoS input rules' and the other for 'QoS output rules', which are for prioritizing inbound and outbound traffic, respectively. Each section lists all the gateway devices on which rules can be set. You can set rules on all devices at once, using the 'All devices' entry.

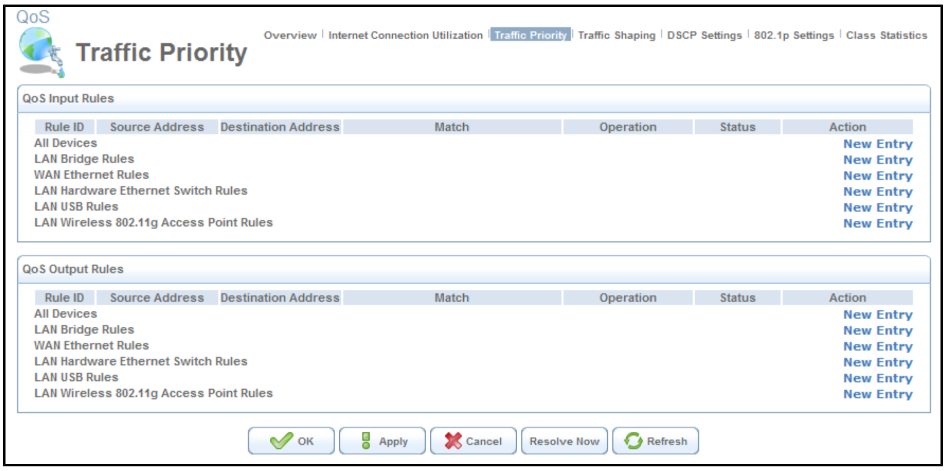


Figure 5.59 Traffic Priority

2. After choosing the traffic direction and the device on which to set the rule, click the appropriate 'New Entry' link. The 'Add Traffic Priority Rule' screen appears.

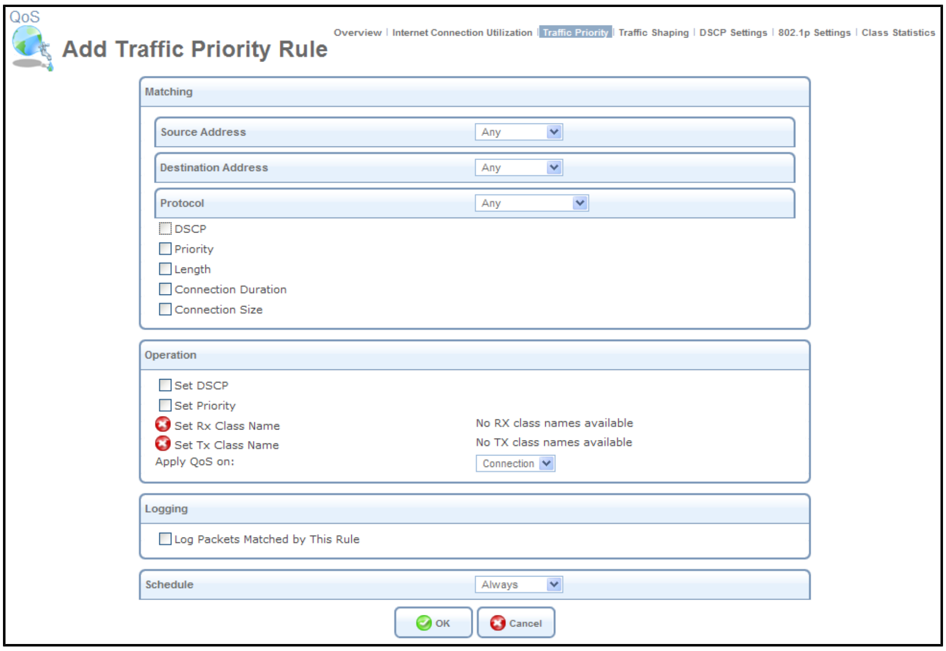


Figure 5.60 Add Traffic Priority Rule

This screen is divided into two main sections, 'Matching' and 'Operation', which are for defining the operation to be executed when matching conditions apply.

Matching Use this section to define characteristics of the packets matching the rule.

- **Source Address** The source address of packets sent or received by OpenRG. Use this drop-down menu to specify the computer or group of computers on which you would like to apply the rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on any host trying to send data. If you would like to add a new address, select the 'User Defined' option in the drop-down menu. This will commence a sequence that will add a new **Network Object**, representing the new host. Refer to Section 6.9.2 in order to learn how to do so.

- **Destination Address** The destination address of packets sent or received by OpenRG. This address can be configured in the same manner as the source address. For example, use this drop-down menu to specify an IP address of a remote application server (such as a security server), which requires that the incoming packets have a specific IP address (e.g., one of those defined in your NAT IP address pool).

- **Protocol** You may also specify a traffic protocol. Selecting the 'Show All Services' option from the drop-down menu expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This will commence a sequence that will add a new **Service**, representing the protocol. Refer to Section 6.9.2 in order to learn how to do so.

  Using a protocol requires observing the relationship between a client and a server, in order to distinguish between the source and destination ports. For example, let's assume you have an FTP server in your LAN, serving clients inquiring from the WAN. You want to apply a QoS rule on incoming packets from any port on the WAN (clients)

trying to access FTP port 21 (your server), and the same for outgoing packets from port 21 trying to access any port on the WAN. Therefore, you must set the following Traffic Priority rules:

- In the 'Matching' section of 'QoS Input Rules', select 'FTP' from the 'Protocol' drop-down menu. The 'TCP Any -> 21' setting appears under 'Ports'.
- Define a priority in the 'Operation' section.
- Click 'OK' to save the settings.
- Define a QoS output rule in the same way as the input rule.

- **DSCP** Select this check box to display two DSCP fields, which enable you to specify a hexadecimal DSCP value and its mask assigned to the packets matching the priority rule. For more information, refer to Section 5.3.5.
- **Priority** Select this check box to display a drop-down menu, in which you can select a priority level assigned to the packets matching the priority rule.
- **Device** Select this check box to display a drop-down menu, in which you can select a network device on which the packet-rule matching will be performed. This option is relevant in case you have previously selected the 'All Devices' option in the 'Traffic Priority' screen (see Figure 5.59).
- **Length** Select this check box if you would like to specify the length of packets, or the length of their data portion.

> Note: The following two options are applicable only if the Fastpath feature is disabled in the 'Routing' menu item under 'System'. Depending on your gateway's model, the feature's name may appear as 'Software Acceleration' or 'Hardware Acceleration'.

- **Connection Duration** Select this check box to apply the priority rule only on connections which are open for a certain time period. This option is especially useful if you would like to accelerate your Web browsing by lowering the speed of concurrently running download jobs, or vice versa. After selecting the check box, choose whether the duration of connections matching the rule should be greater or less than the time that you specify in the adjacent field.

Figure 5.61 Connection Duration

For example, if you define the connection duration as less than 10 seconds, you will notice acceleration of your Web browsing and small file downloads, but slowing down of your large file downloads. The reason for this is that when a connection passes the specified time limit (as in case of a large file download), its priority is lowered, thereby giving more priority to shorter connections.

- **Connection Size** Select this check box to apply the priority rule only on connections matching a certain data size limit. This option is best used along with the 'Connection Duration' option, enabling you to fine-tune the gateway's traffic priority mechanism according to your needs. After selecting the check box, choose whether the connection's data size should be greater or less than the number of kilobytes that you specify in the adjacent field.

Figure 5.62 Connection Size

For example, if you define the connection size as less than 400 kilobytes, you will notice acceleration of Web browsing, and lowering of your file download speed. The reason for this is that when a connection exceeds the specified data size limit, its priority is lowered, thereby giving more priority to connections with a smaller data size.

Operation Perform the following operation/s on packets that match the priority rule.

- **Set DSCP** Select this check box if you would like to change the DSCP value on packets matching the rule, prior to routing them further. The screen refreshes (see Figure 5.63), enabling you to enter the hexadecimal DSCP value in its respective field that appears.

Figure 5.63 Set DSCP Rule

- **Set Priority** Select this check box if you would like to change a priority of the packets matching the rule. The screen refreshes (see Figure 5.64), enabling you to select between one of eight priority levels, zero being the lowest and seven the highest. Each priority level is assigned a default queue number, where Queue 0 has the lowest priority. OpenRG's QoS supports up to eight queues.

Figure 5.64 Set Priority with Queueing

The matching between a priority level and a queue number can be edited in the '802.1p Settings' screen (for more information, refer to Section 5.3.6).

- **Apply QoS on** Select whether to apply QoS on a connection or just the first packet. When applying on a connection, the data transfer session will be handled using Stateful Packet Inspection (SPI). This means that other packets matching this rule will be automatically allowed to access, and the same QoS scheme will be applied to them.

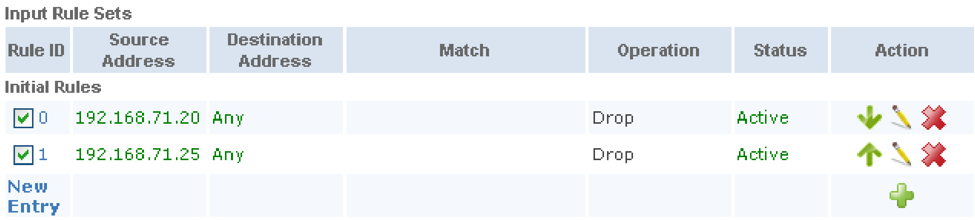
Logging Monitor the rule.

- **Log Packets Matched by This Rule** Select this check box to log the first packet from a connection that was matched by this rule.

Schedule By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

3. Click 'OK' to save the settings.

The order of the rules' appearance represents both the order in which they were defined and the sequence by which they will be applied. You may change this order after your rules are already defined (without having to delete and then re-add them), by using the action icon and action icon .



Input Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Initial Rules						
0	192.168.71.20	Any		Drop	Active	
1	192.168.71.25	Any		Drop	Active	
New Entry						

Figure 5.65 Move Up and Move Down Action Icons

5.3.4 Avoiding Congestion with Traffic Shaping

Traffic Shaping is the solution for managing and avoiding congestion where a high speed LAN meets limited broadband bandwidth. In the scenario of a 100 Mbps Ethernet LAN with a 100 Mbps WAN interface gateway, the gateway may have to communicate with the ISP using a modem with a bandwidth of 2Mbps. This typical configuration makes the modem, having no QoS module, the bottleneck.

Instead of sending traffic as fast as it is received, OpenRG's QoS algorithms perform traffic shaping, limiting the bandwidth of the gateway, thus artificially forcing it to become the bottleneck. A traffic shaper is essentially a regulated queue that accepts uneven and/or bursty flows of packets and transmits them in a steady, predictable stream so that the network is not overwhelmed with traffic. While Traffic Priority allows basic prioritization of packets, Traffic Shaping provides more sophisticated definitions, such as:

- Bandwidth limit for each device
- Bandwidth limit for classes of rules
- Prioritization policy
- TCP serialization on a device

Additionally, you can define QoS traffic shaping rules for a default device. These rules will be used on a device that has no definitions of its own. This enables the definition of QoS rules on

Default WAN, for example, and their maintenance even if the PPP or bridge device over the WAN is removed.

5.3.4.1 Shaping the Traffic of a Device

To shape the traffic of a device, perform the following:

1. Click 'Traffic Shaping' under the QoS tab in the 'Services' screen. The 'Traffic Shaping' screen appears.

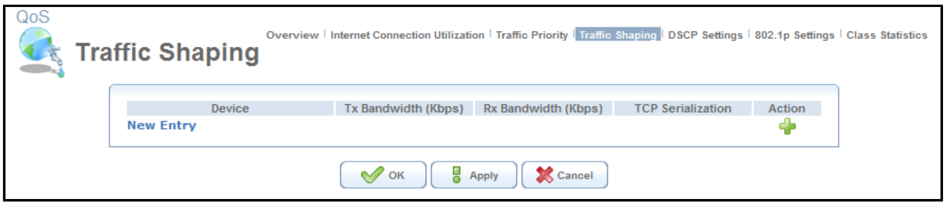


Figure 5.66 Traffic Shaping

2. Click the 'New Entry' link. The 'Add Device Traffic Shaping' screen appears (see Figure 5.67).

3. Select the device for which you would like to shape the traffic. The drop-down menu includes all your gateway's devices, and you can select either a specific device for which to shape the traffic, or 'Any Device' to add a traffic class to all devices. In this example, select the WAN Ethernet option.

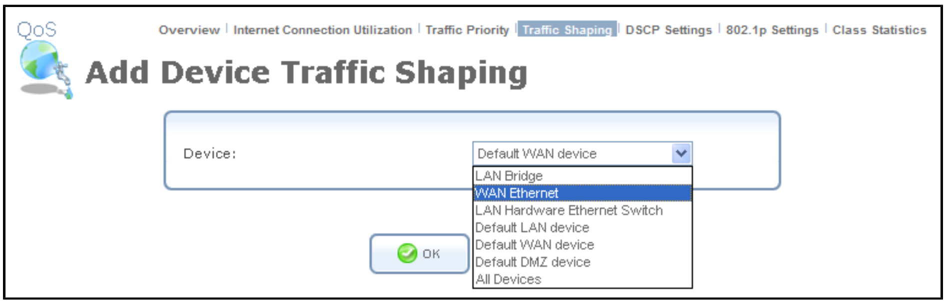


Figure 5.67 Add Device Traffic Shaping

> If you would like to configure OpenRG's LAN traffic transmission/reception rate, select the relevant LAN device. If you would like to apply the settings on all LAN devices, select the 'Default LAN Device' entry.

4. Click 'OK'. The 'Edit Device Traffic Shaping' screen appears.

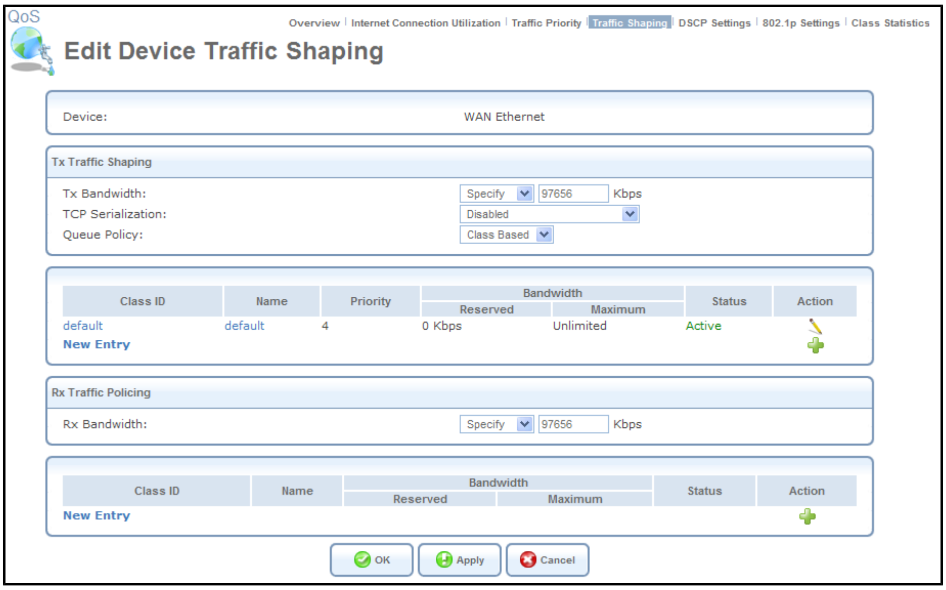


Figure 5.68 Edit Device Traffic Shaping

5. Configure the following fields:

Tx Bandwidth This parameter limits the gateway's bandwidth transmission rate. The purpose is to limit the bandwidth of the WAN device to that of the weakest outbound link, for instance, the DSL speed provided by the ISP. This forces OpenRG to be the network bottleneck, where sophisticated QoS prioritization can be performed. If the device's bandwidth is not limited correctly, the bottleneck will be in an unknown router or modem on the network path, rendering OpenRG's QoS useless.

TCP Serialization You can enable TCP Serialization in its drop-down menu, either for active voice calls only or for all traffic. The screen will refresh, adding a 'Maximum Delay' field (see Figure 5.69). This function allows you to define the maximal allowed transmission time frame (in milliseconds) of a single packet. Any packet that requires a longer time to be transmitted, will be fragmented to smaller sections. This avoids transmission of large, bursty packets that may cause delay or jitter for real-time traffic such as VoIP. If you insert a delay value in milliseconds, the delay in number of bytes will be automatically updated on refresh.

Figure 5.69 TCP Serialization – Maximum Delay

Queue Policy Tx traffic queueing can be based on a traffic class (see the following explanations) or on the pre-defined priority levels (refer to Section 5.3.3). Note that when it is based on a traffic class, the class's bandwidth requirements will be met regardless of the priority, and only excess bandwidth will be given to traffic with a higher priority. However, when unlimited bandwidth is selected for the Tx traffic, the queue policy can only be based on the pre-defined priority levels.

5.3.4.2 Creating a Traffic Shaping Class

The bandwidth of a device can be divided in order to reserve constant portions of bandwidth to predefined traffic types. Such a portion is known as a *Traffic Shaping Class*. When not used by its predefined traffic type, or owner (for example VoIP), the bandwidth will be available to all other traffic. However when needed, the entire class is reserved solely for its owner.

Moreover, you can limit the maximum bandwidth that a class can use even if the entire bandwidth is available. When a traffic class is first defined for a specific traffic type, two classes are created. The second class is the 'Default Class', which is responsible for all the packets that *do not* match the defined traffic class, or any other classes that may be defined on the device. You can also define **wildcard** devices, such as all WAN devices. This can be viewed in the 'Class Statistics' screen (see Figure 5.79).

To define a new traffic shaping class, perform the following:

1. In the 'Edit Device Traffic Shaping' screen (see Figure 5.68), click the 'New Entry' link in the 'Tx Traffic Shaping' section. The 'Add Shaping Class' screen appears.

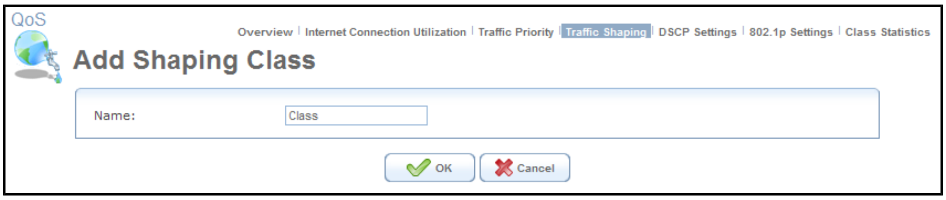


Figure 5.70 Add Shaping Class

2. Name the new class and click 'OK' to save the settings, e.g. Class A.

3. Back in the 'Edit Device Traffic Shaping' screen, click the class name to edit the traffic class. Alternatively, click its action icon . The 'Edit Shaping Class' screen appears.

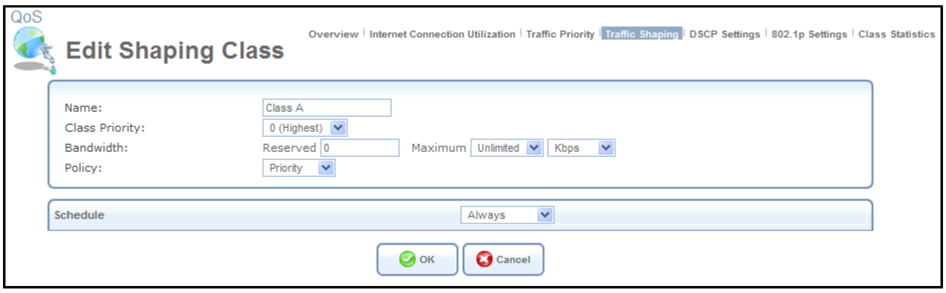


Figure 5.71 Edit Shaping Class

4. Configure the following fields:

Name The name of the class.

Class Priority The class can be granted one of eight priority levels, zero being the highest and seven the lowest (note the obversion when compared to the rules priority levels). This level sets the priority of a class in comparison to other classes on the device.

Bandwidth The reserved transmission bandwidth in kilo-bits per second. You can limit the maximum allowed bandwidth by selecting the 'Specify' option in the drop-down menu. The screen will refresh, adding another Kbits/s field.

Figure 5.72 Specify Maximum Bandwidth

Policy The class policy determines the policy of routing packets inside the class. Select one of the four options:

- **Priority** Priority queuing utilizes multiple queues, so that traffic is distributed among queues based on priority. This priority is defined according to packet's priority, which can be defined explicitly, by a DSCP value (refer to Section 5.3.5), or by a 802.1p value (refer to Section 5.3.6).
- **FIFO** The "First In, First Out" priority queue. This queue ignores any previously-marked priority that packets may have.
- **Fairness** The fairness algorithm ensures no starvation by granting all packets a certain level of priority.
- **RED** The Random Early Detection algorithm utilizes statistical methods to drop packets in a "probabilistic" way before queues overflow. Dropping packets in this way slows a source down enough to keep the queue steady and reduces the number of packets that would be lost when a queue overflows and a host is transmitting at a high rate.
- **WRR** Weighted Round Robin utilizes a process scheduling function that prioritizes traffic according to the pre-defined 'Weight' parameter of a traffic's class. This level of prioritizing provides more flexibility in distributing bandwidth between traffic types, by defining additional classes within a parent class.

Schedule By default, the class will always be active. However, you can configure scheduler rules in order to define time segments during which the class may be active. To learn how to configure scheduler rules, refer to the 'Defining Scheduler Rules' section of the OpenRG Administrator Manual.

5.3.4.3 Setting an Incoming Traffic Policy

When shaping the traffic for a device, you must also determine a policy for incoming traffic. In the 'Edit Device Traffic Shaping' screen (see Figure 5.68), configure the following fields in the 'Rx Traffic Policing' section:

Rx Bandwidth This parameter limits the device's bandwidth reception rate. In this example, the purpose is to limit the bandwidth that the WAN device can receive from the ISP.

Queue Policy Similar to Tx traffic, Rx traffic queueing can be based on a traffic class or on strict priority (unless unlimited bandwidth is selected). By default, however, the queue policy is set to Policer, which is a relatively simple method of bandwidth control. With the policer

option, you can dedicate a portion of the bandwidth to a certain traffic type. This portion will always remain available to its traffic type, even when not in use. This is a simpler method, as prioriy is not used at all.

When selecting a class-based queue policy, you must define an Rx Traffic Policy Class, which is identical to defining a Tx Traffic Shaping Class, described earlier. However if you select the policer as your queue policy, defining a policing class is even simpler, as it lacks the priority setup.

To define an Rx traffic policy class, perform the following:

1. In the 'Edit Device Traffic Shaping' screen (see Figure 5.68), click the 'New Entry' link in the 'Rx Traffic Policing' section. The 'Add Policing Class' screen appears.

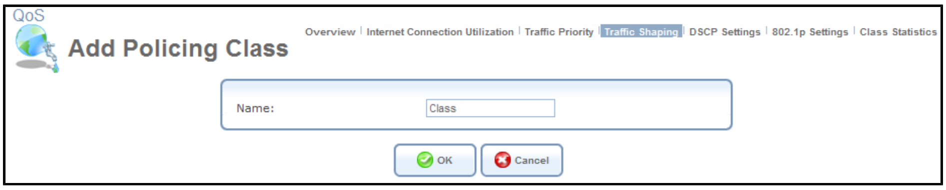


Figure 5.73 Add Policing Class

2. Name the new class and click 'OK' to save the settings, e.g. Class B.

3. Back in the 'Edit Device Traffic Shaping' screen, click the class name to edit the traffic class. Alternatively, click its action icon . The 'Edit Policing Class' screen appears.

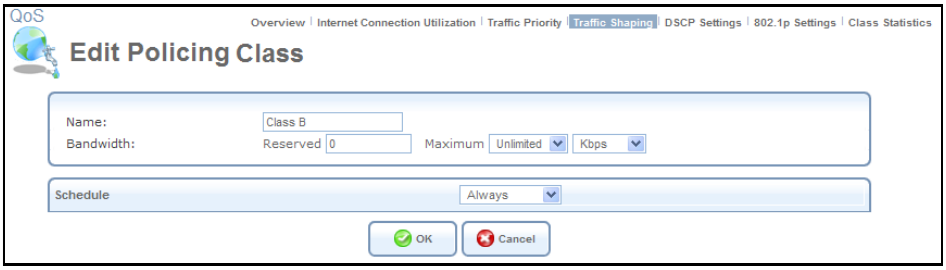


Figure 5.74 Edit Policing Class

Configure the following fields:

Name The name of the class.

Bandwidth The reserved reception bandwidth in kilo-bits per second. You can limit the maximum allowed bandwidth by selecting the 'Specify' option in the combo box. The screen refreshes, adding yet another Kbps field.

Figure 5.75 Specify Maximum Bandwidth

Schedule By default, the class will always be active. However, you can configure scheduler rules in order to define time segments during which the class may be active. To learn how

to configure scheduler rules, refer to the 'Defining Scheduler Rules' section of the OpenRG Administrator Manual.

5.3.5 Prioritizing Traffic with DSCP

In order to understand what is Differentiated Services Code Point (DSCP), one must first be familiarized with the *Differentiated Services* model. Differentiated Services (Diffserv) is a Class of Service (CoS) model that enhances best-effort Internet services by differentiating traffic by users, service requirements and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service, as appropriate for voice calls, video playback or other delay-sensitive applications, via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.

Diffserv defines a field in IP packet headers referred to as DSCP. Hosts or routers passing traffic to a Diffserv-enabled network will typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply particular queue handling or scheduling behavior. OpenRG provides a table of predefined DSCP values, which are mapped to 802.1p priority marking method (refer to Section 5.3.6).

You can edit or delete any of the existing DSCP setting, as well as add new entries.

1. Under the QoS menu item, click 'DSCP Settings'. The following screen appears.

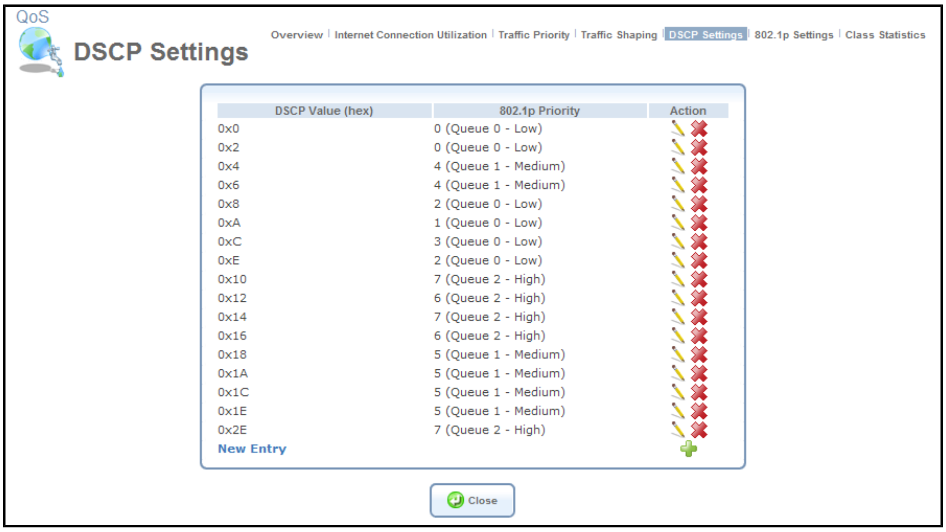


Figure 5.76 DSCP--Traffic Priority Matching

Each DSCP value is assigned a default queue number as a part of its 802.1p priority settings. OpenRG's QoS supports up to eight queues, where Queue 0 has the lowest priority.

2. To edit an existing entry, click its action icon . To add a new entry, click the 'New Entry' link. In both cases, the 'Edit DSCP Settings' screen appears.

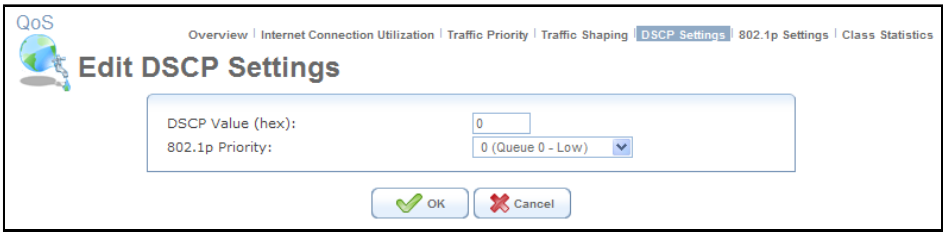


Figure 5.77 Edit DSCP Settings

3. Configure the following fields:

   DSCP Value (hex) Enter a hexadecimal number that will serve as the DSCP value.

   802.1p Priority Select a 802.1p priority level from the drop-down menu (each priority level is mapped to low/medium/high priority).

4. Click 'OK' to save the settings.

> Note: The DSCP value overriding the priority of incoming packets with an unassigned value (priority 0, assumed to be a no-priority-set) is "0x0".

5.3.6 Configuring 802.1p Priority Values

The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/MAC sub-layer. 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established. The 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority (0-7), where level 7 is the highest one. In addition, OpenRG maps these eight levels to priority queues, where Queue 0 has the lowest priority.

OpenRG's QoS supports up to eight queues. By default, the higher the level and queue values, the more priority they receive. Therefore, the more critical the traffic is, the higher priority level and queue number it should receive. To change the mapping between a priority value and a queue value, perform the following:

1. Under the 'QoS' menu item, click '802.1p Settings'. The following screen appears.

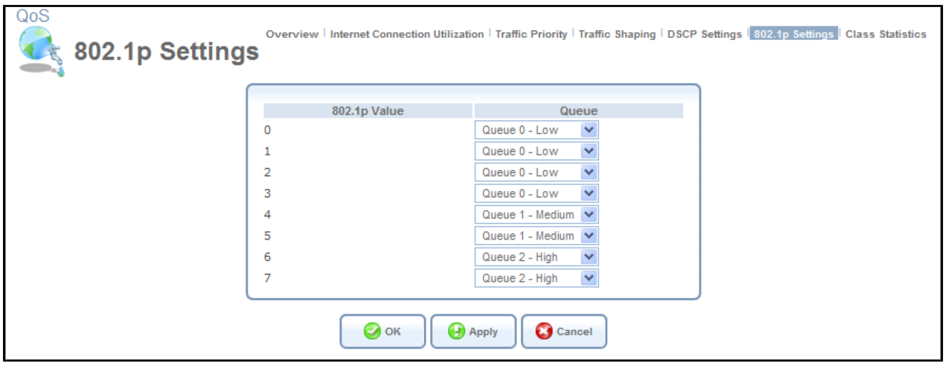


Figure 5.78 Traffic Queuing in 802.1p Settings

2. From the corresponding drop-down menu, select a desired value.

3. Click 'OK' to save the settings.

5.3.7 Viewing Traffic Statistics

OpenRG provides you with accurate, real-time information on the traffic moving through your defined device classes. For example, the amount of packets sent, dropped or delayed, are just a few of the parameters that you can monitor per each shaping class. To view your class statistics, click 'Class Statistics' under the QoS menu item. The following screen appears.

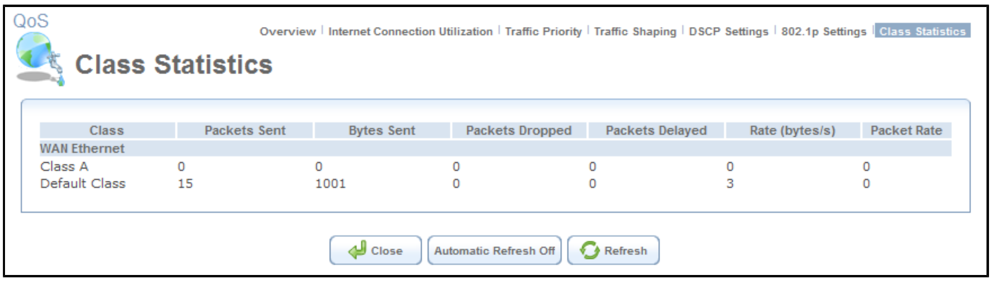


Figure 5.79 Class Statistics

Note that class statistics will only be available after defining at least one class (otherwise the screen will not present any information).

5.3.8 Example: Providing Priority to a Voice Stream

In order to gain a better understanding of the Quality of Service concept, this section presents a scenario where the WAN bandwidth is shaped to provide priority to a voice stream. When shared by a Voice over IP (VoIP) conversation and a file transfer, the bandwidth will normally be exploited by the file transfer, reducing the quality of the conversation or even casuing it to disconnect. With QoS, the VoIP conversation, which is a real-time session, receives the priority it requires, maintaining a high level of voice quality.

5.3.8.1 Hardware Requirements

- A gateway runnning OpenRG
- Two IP phones
- A LAN computer running an FTP client, containing a large file (100MB)
- A WAN computer running an FTP server

5.3.8.2 Physical Setup

1. Connect an IP phone and the LAN computer to OpenRG's LAN ports.

2. Connect OpenRG's WAN port to your network. The second IP phone and the WAN computer should be available on the WAN.

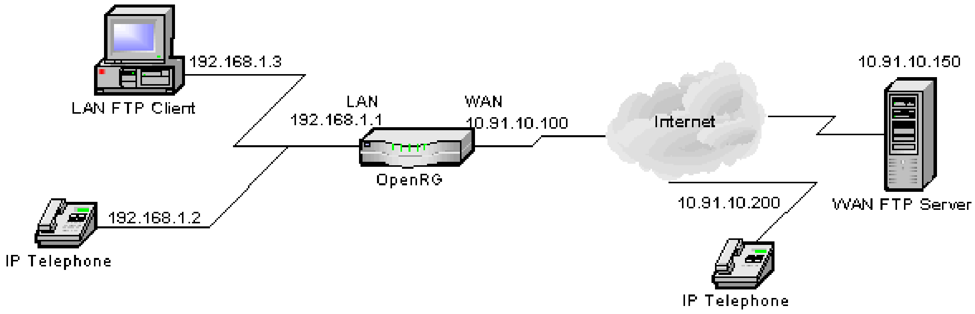


Figure 5.80 Physical Setup

5.3.8.3 Scenario Configuration

1. Configure OpenRG and all other devices with the static IPs described in Figure 5.80.
2. Define a global service for the VoIP stream over a SIP protocol:

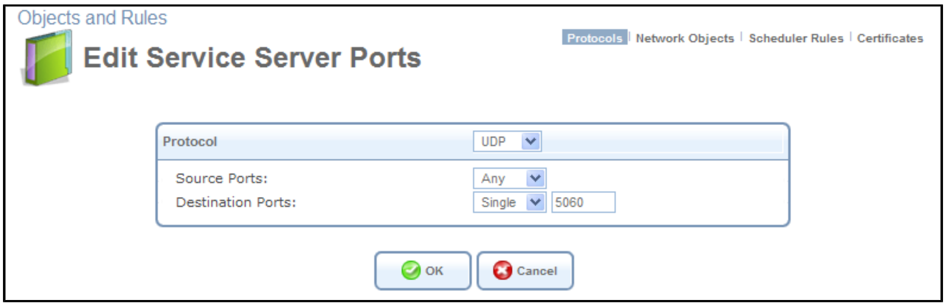


Figure 5.82 Edit Service Server Ports

   a. In OpenRG's WBM, click the 'Protocols' icon in the 'Advanced' screen, and then click the 'New Entry' link. The 'Edit Service' screen appears (see Figure 5.81).
   b. Enter "SIP" as the service name. You may also add a description for the service.

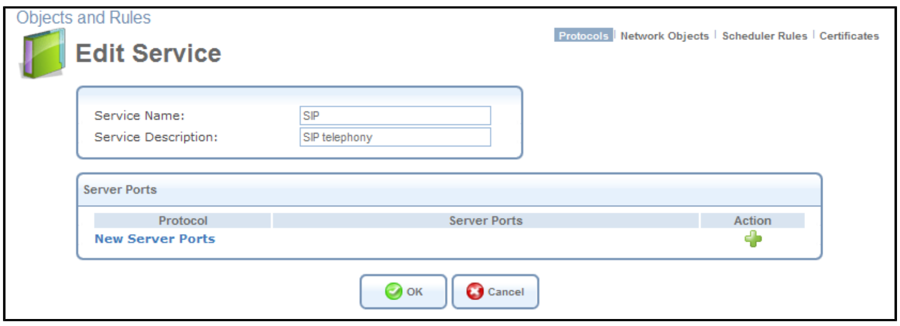


Figure 5.81 Edit Service

   c. Click the 'New Server Ports' link. The 'Edit Service Server Ports' screen appears (see Figure 5.82).

d. From the drop-down menu, select the UDP protocol. The screen will refresh.

e. Verify that "Any" is selected from the 'Source Ports' drop-down menu.

f. From the 'Destination Ports' drop-down menu, select "Single". The screen will refresh again.

g. Enter 5060 as the single destination port.

h. Click 'OK' to save the settings.

3. Limit the bandwidth of OpenRG's WAN device:

a. Under the 'QoS' menu item, click 'Traffic Shaping'. The following screen appears.

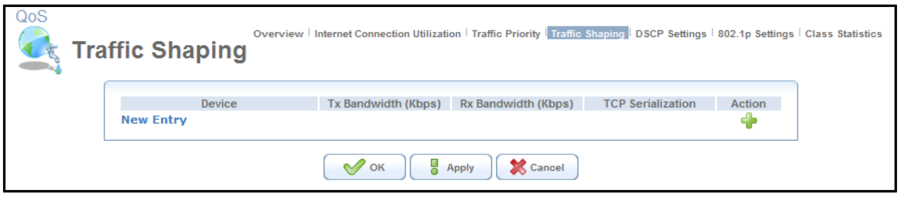


Figure 5.83 Traffic Shaping

b. Click the 'New Entry' link, and select 'All Devices' from the drop-down menu.

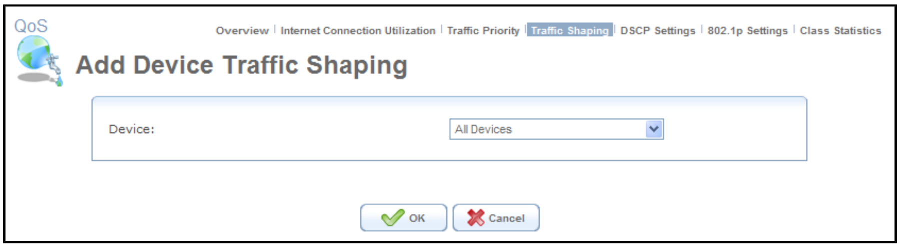


Figure 5.84 Add Device Traffic Shaping

c. Click 'OK'. The 'Edit Device Traffic Shaping' screen appears.

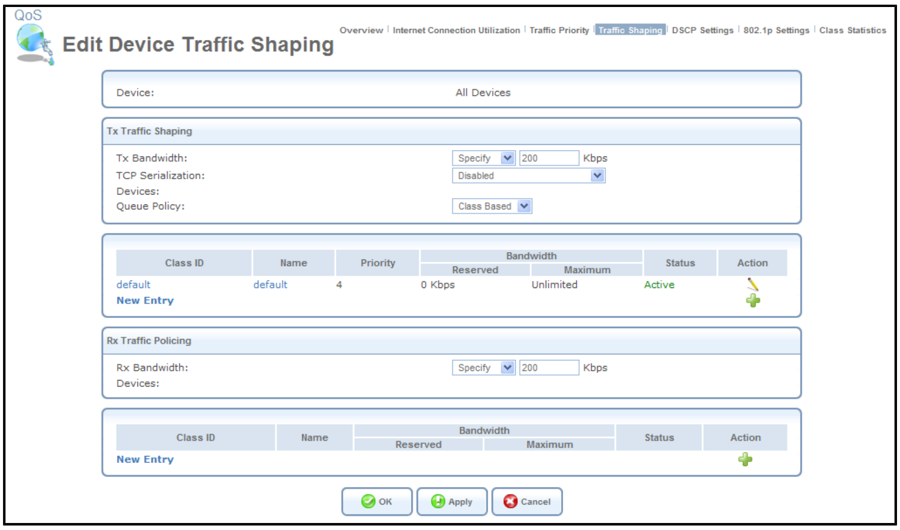


Figure 5.85 Edit Device Traffic Shaping

d. In the Tx Bandwidth drop-down menu, select 'Specify', and enter 200 Kbps in the field that appears.

e. In the Rx Bandwidth drop-down menu, select 'Specify', and enter 200 Kbps in the field that appears.

f. Verify that TCP Serialization is disabled.

4. Configure a QoS class for the Tx and Rx VoIP streams. Perform this procedure twice: once for Tx Traffic Shaping and once for Rx Traffic Policing.

   a. Click the 'New Entry' link in the Tx/Rx traffic shaping section of the 'Edit Device Traffic Shaping' screen. The 'Add Class' screen appears (see Figure 5.86).

   b. Name the new class "VoIP Tx/Rx", and click 'OK' to save the settings.

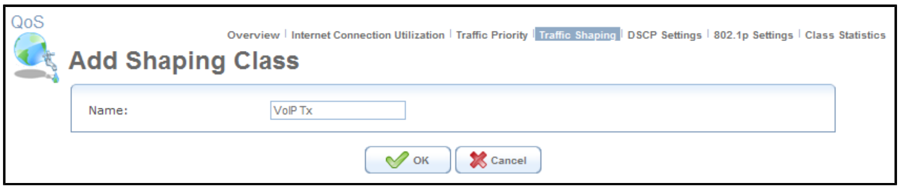


Figure 5.86 Add Shaping Class

   c. Uncheck the entry in the Class ID column to disable the class at this point (see Figure 5.87).

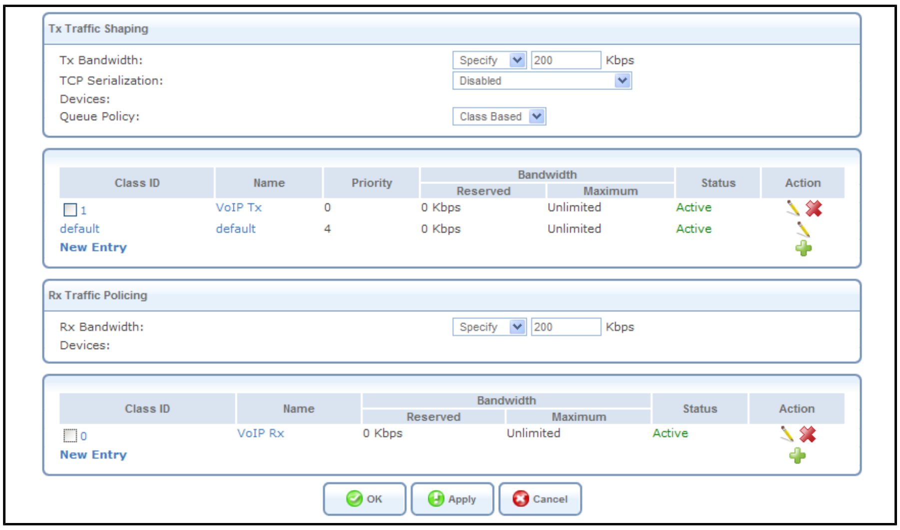


Figure 5.87 Shaping Classes – Uncheck the Class ID

d. Click the class name to edit the shaping class. Alternatively, click its action icon . The 'Edit Class' screen appears (see Figure 5.88).

e. Enter 100 Kbps in the Reserved Tx/Rx Bandwidth field.

f. Leave all other fields at their default values.

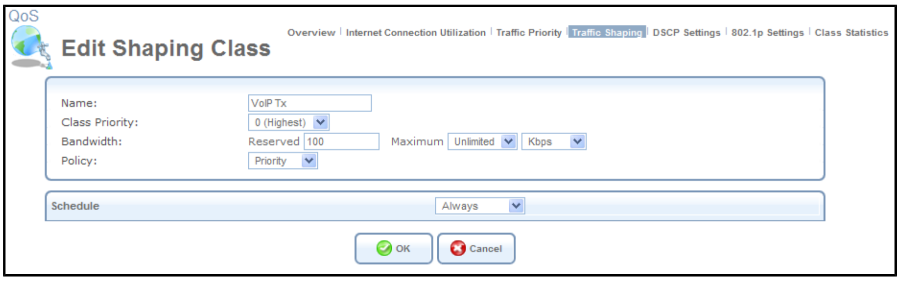


Figure 5.88 Edit Shaping Class

g. Click 'OK' to save the settings.

h. Click 'OK' once more in the 'Edit Device Traffic Shaping' screen to save all settings.

5. Define and associate class rules:

a. Click 'Traffic Priority' under the 'QoS' tab in the 'Services' screen. The 'Traffic Priority' screen appears.

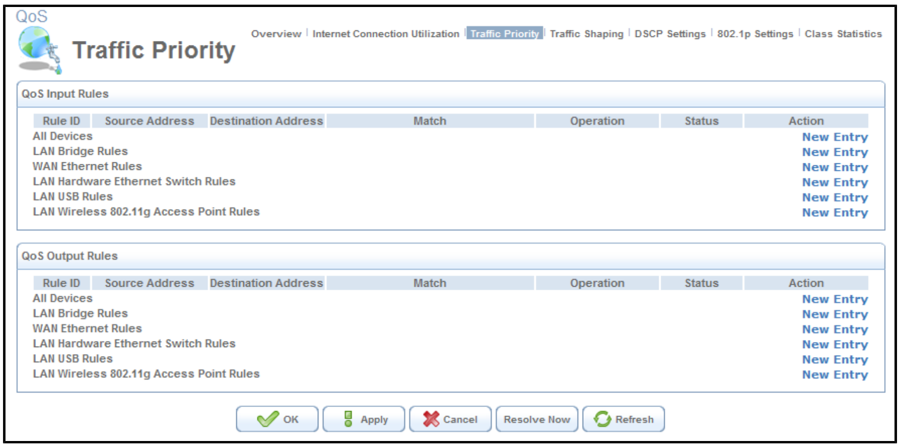


Figure 5.89 Traffic Priority

b. Click the 'New Entry' link of the 'WAN Ethernet Rules' under the 'QoS Output Rules' section. The 'Add Traffic Priority Rule' screen appears.

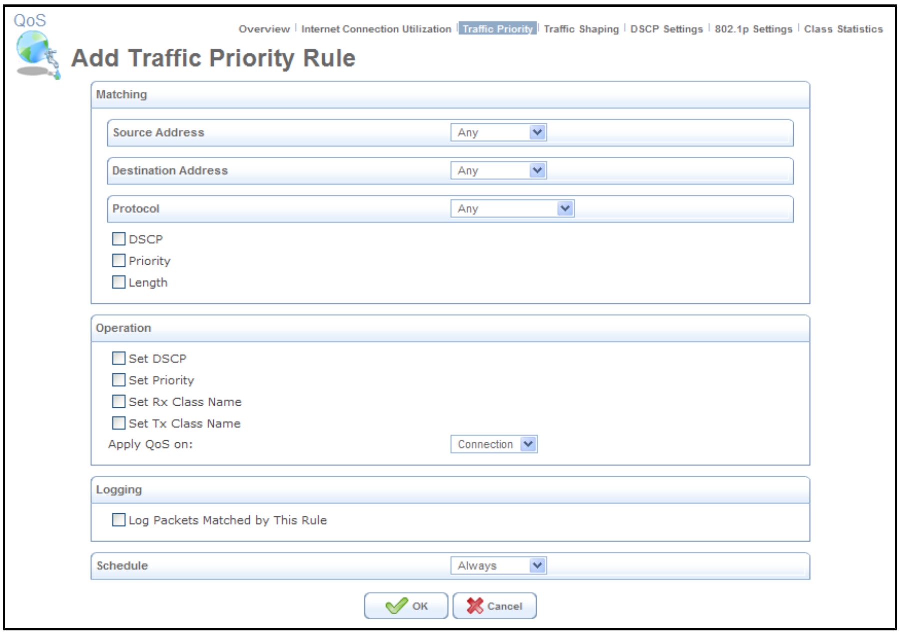


Figure 5.90 Add Traffic Priority Rule

c. In the 'Matching' section, select 'Show All Services' from the 'Protocol' drop-down menu, and then select "SIP". The screen will refresh displaying the protocol parameters (see Figure 5.91).

d. In the 'Operation' section, check the 'Set Rx/Tx Class Name' check boxes, and select 'VoIP Rx/Tx' from the drop-down menus that appear.

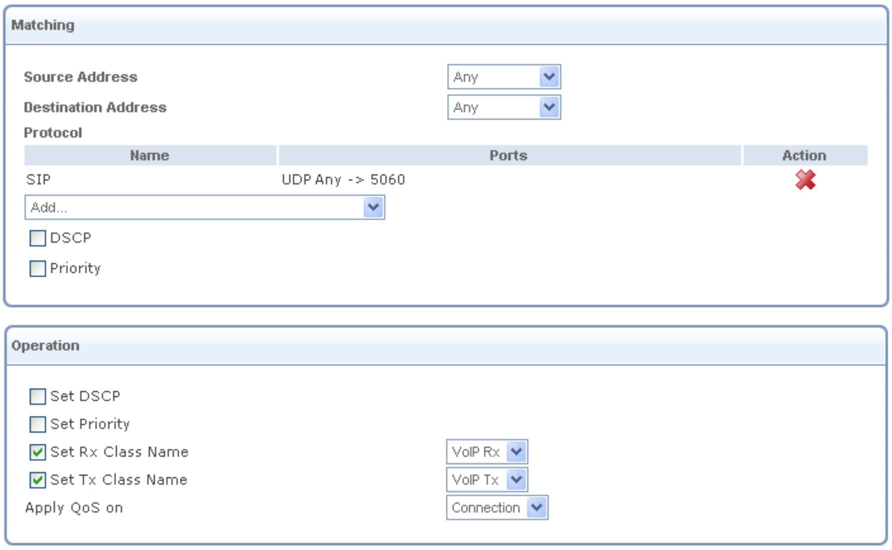


Figure 5.91 Add Traffic Priority Rule – SIP Protocol

e. Leave all other fields at their default values, and click 'OK' to save the settings.

5.3.8.3.1 Implementing the WRR Class Policy in VoIP's QoS

The WRR class policy enables you to fine-tune your Tx traffic priority settings. For instance, in a scenario where you utilize more than one VoIP protocol (for example, SIP and H.323), you can further prioritize VoIP's Tx traffic. In the following example, the SIP protocol is given preference over H.323. Therefore, you may assign 70% of the VoIP bandwidth to the SIP-based traffic, and 30% to the H.323-based traffic. To enable the WRR class policy, perform the following:

1. In the 'Edit Device Traffic Shaping' screen (see Figure 5.87), click the 'VoIP Tx' link. The 'Edit Shaping Class' screen appears (see Figure 5.88).

2. From the 'Policy' drop-down menu, select the WRR option. The screen refreshes, and a new section called 'Subclasses' is added.

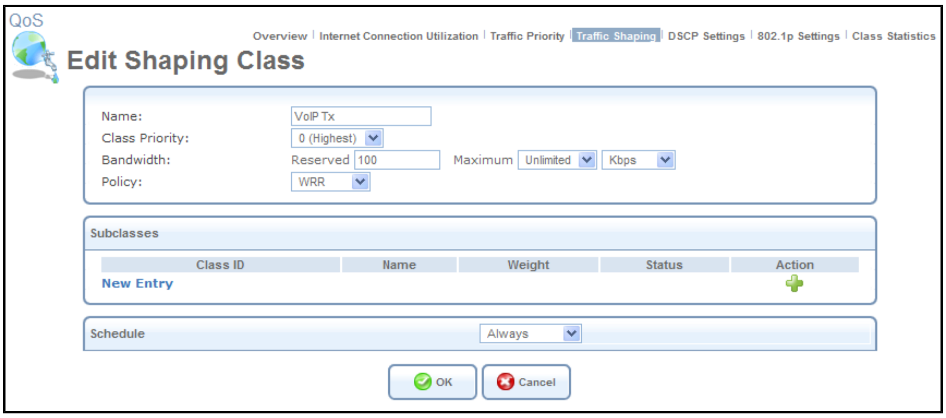


Figure 5.92 Subclasses Section in Edit Shaping Class

3. In the 'Subclasses' section, click either the 'New Entry' link or the action icon . The 'Add Shaping Class' screen appears.

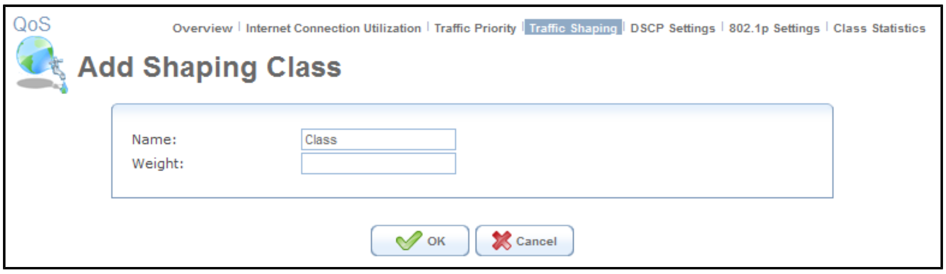


Figure 5.93 Add Shaping Class

This time, the screen contains two fields: 'Name' and 'Weight'.

4. In the 'Name' field, enter 'SIP' for the name of a VoIP's subclass assigned to the SIP-based traffic.

5. In the 'Weight' field, enter a numeric value that correlates with the amount of bandwidth you want to grant to the subclass. In the current example, the subclass is granted 70% of VoIP's Tx traffic. Therefore, enter **7** in the 'Weight' field.

> Note: The class weight range is between 1 and 10000.

6. Click 'OK' to save the settings.

Repeat the same procedure for creating the H.323 subclass of VoIP. However, in the 'Weight' field enter **3** that corresponds to 30% of the VoIP bandwidth you want to assign to the H.323 subclass.

> Note: When you activate the WRR class policy, it is not mandatory to define an Rx shaping class and its priority rules.

Once the subclasses are created, define the priority rules for the subclasses, as follows:

1. Click 'Traffic Priority' under the 'QoS' tab in the 'Services' screen. The 'Traffic Priority' screen appears (see Figure 5.89).

2. Click the 'New Entry' link of the 'WAN Ethernet Rules' under the 'QoS Output Rules' section. The 'Add Traffic Priority Rule' screen appears (see Figure 5.90).

3. In the 'Matching' section, select 'Show All Services' in the 'Protocol' drop-down menu, and then select 'SIP'. The screen refreshes displaying the protocol parameters.

> Note: You can also define the 'SIP' protocol manually, as described in Section 5.3.8.3.

4. In the 'Operation' section, check the 'Set Tx Class Name' check box, and select 'SIP' in the drop-down menu that appears.

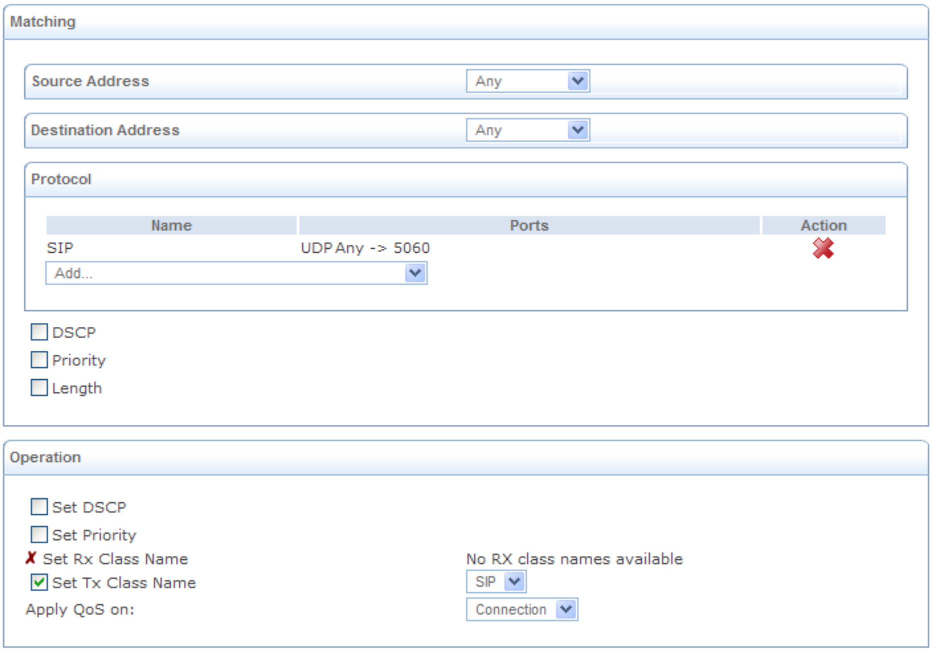


Figure 5.94 Add Traffic Priority Rule # SIP Protocol

5. Leave all other fields at their default values, and click 'OK' to save the settings.

Repeat the same procedure for defining a priority rule for the H.323 subclass. The only difference is that you should select the 'H.323 Call Signaling' value for the protocol settings, and 'H.323' for the Tx class name.

5.3.8.4 Running the Scenario

1. Initiate a direct call (using the SIP protocol) from one IP phone to the other. For VoIP configuration, refer to Section 5.5. Verify that the conversation can be conducted clearly and adequately.

2. Initiate an FTP file upload from the LAN computer to the WAN computer. This can be done using the Windows command line. Use the **hash** command to utilize the pound sign process indicator before starting the file transfer. As soon as the upload commences, your ability to transmit voice will be lost—the WAN party will not be able to hear you. The upload, on the other hand, will be proceeding rapidly, taking up all of your transmit bandwidth (see Figure 5.95).

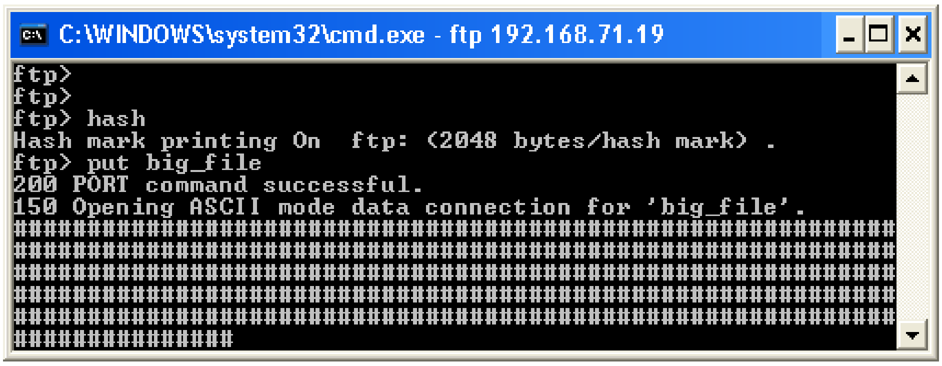


Figure 5.95 FTP Process

3. Activate QoS to restore the voice transmission:

   a. Under the 'QoS' menu item, click 'Traffic Shaping'. The 'Traffic Shaping' screen appears.

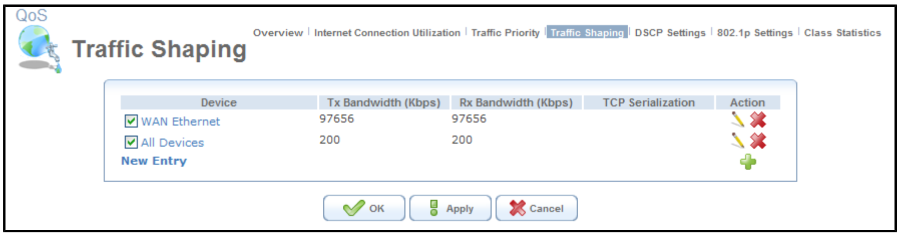


Figure 5.96 Traffic Shaping

   b. Click the Device name, in this case 'All devices', and check both entries in the Class ID column to enable the classes (see Figure 5.97).

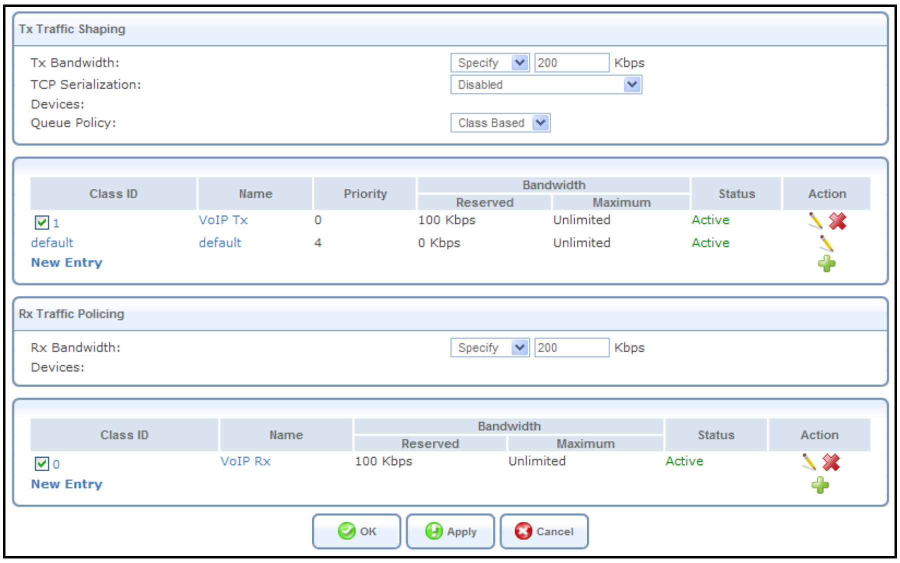


Figure 5.97 Shaping Classes – Check the Class ID

   c. Click 'OK' to save the settings.

The transmission capability will be restored, as most of the bandwidth will now be reserved for the VoIP stream. The file upload rate, on the other hand, will obviously slow down.

> Note: Some IP phones and ATA devices are preconfigured to send DSCP-marked data. OpenRG will handle such data with QoS priority, even if a QoS class is not configured for the VoIP stream. To run the above scenario successfully, you must first disable DSCP marking on such devices.

5.3.9 Example: Providing Priority to an IPTV Stream

This section presents a scenario in which the WAN bandwidth is shaped to provide priority to a media broadcast (for example, an IPTV stream). When your bandwidth is shared between a media stream and data transfer, a greater portion of it will normally be used by the data transfer, reducing the quality of the media broadcast or even disrupting it. With the help of OpenRG's Traffic Shaping feature, the media stream receives the priority it requires, thereby maintaining its quality. This scenario is based on the following real-life case.

Assume that you have a 100 Mbps Ethernet LAN with a 100 Mbps WAN interface router. The router communicates with the ISP network via a modem that has a 2Mbps bandwidth, and does not have a QoS module. When OpenRG's Traffic Shaping feature is disabled, the router sends traffic to the modem as fast as it is received from the LAN host. This typical configuration makes the modem a bottleneck. However, if you enable Traffic Shaping on the router, it will limit the router's bandwidth, artificially forcing it to be the bottleneck. This configuration creates a regulated traffic queue that enables the router to accept uneven and bursty flows of packets and transmit them in a steady, predictable stream.

5.3.9.1 Simulating Limited Bandwidth and IPTV Setup

As a first step, simulate limited bandwidth by reducing OpenRG's Rx/Tx bandwidth in the following way:

1. Under the 'Services' tab, click 'QoS'. The following screen appears.

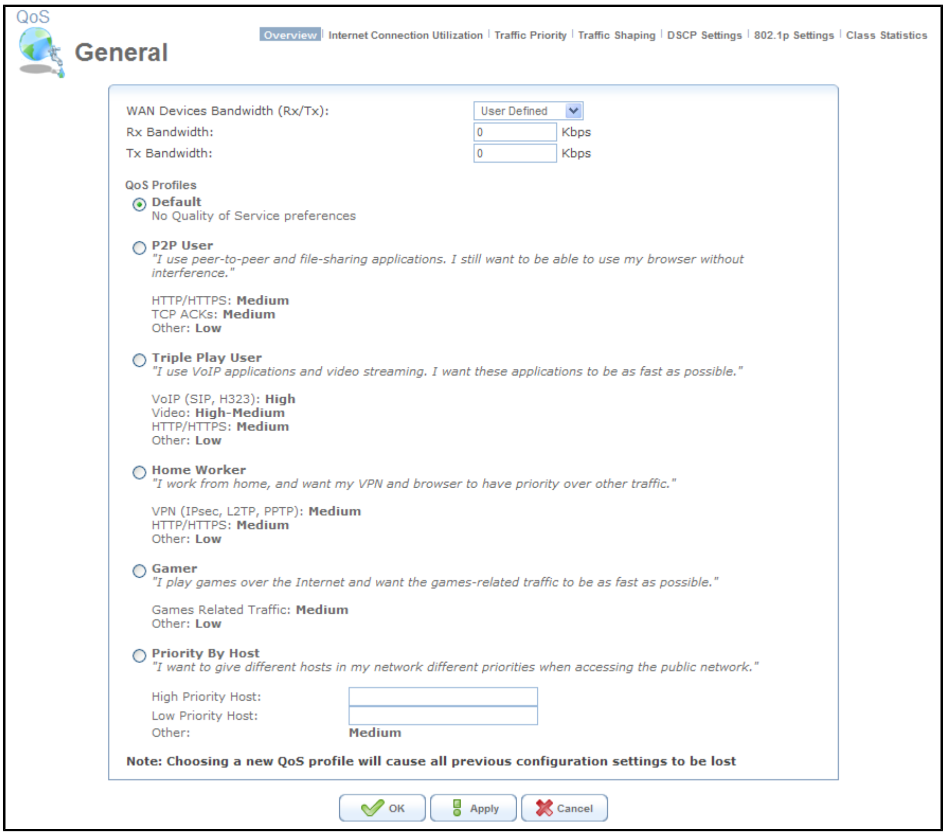


Figure 5.98 General

2. From the 'WAN Devices Bandwidth(Rx/Tx)' drop-down menu, select 5000/256 Kbps.

3. Click 'OK' to save the settings.

To simulate an IPTV setup, use the *Video LAN Client* (VLC) application. VLC supports both Client and Server modes. In its server mode, VLC can be used on a WAN host as the broadcaster, which sends a video stream to a multicast group. In its client mode, VLC can be used as a media player on a LAN host. VLC uses a multicast IP address range between 224.0.0.0 – 239.255.255.255. It can be installed both on Linux and Windows computers. You can download VLC from http://www.videolan.org/vlc/download-windows.html.

To configure the VLC server, perform the following:

1. In VLC's 'File' menu, select 'Wizard'. The following screen appears.

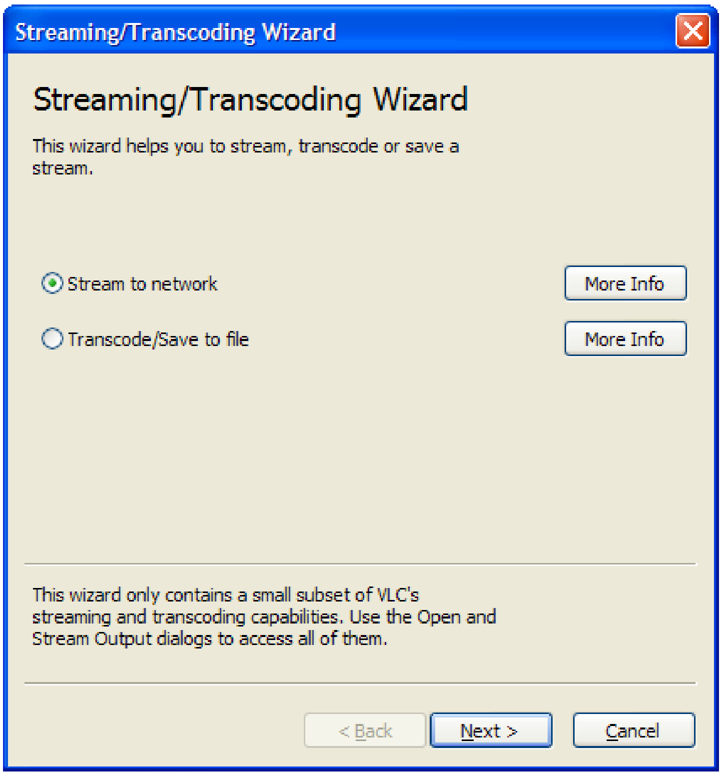


Figure 5.99 Streaming/Transcoding Wizard

2. Select the 'Stream to Network' radio button and click 'Next'. The 'Input' screen appears.

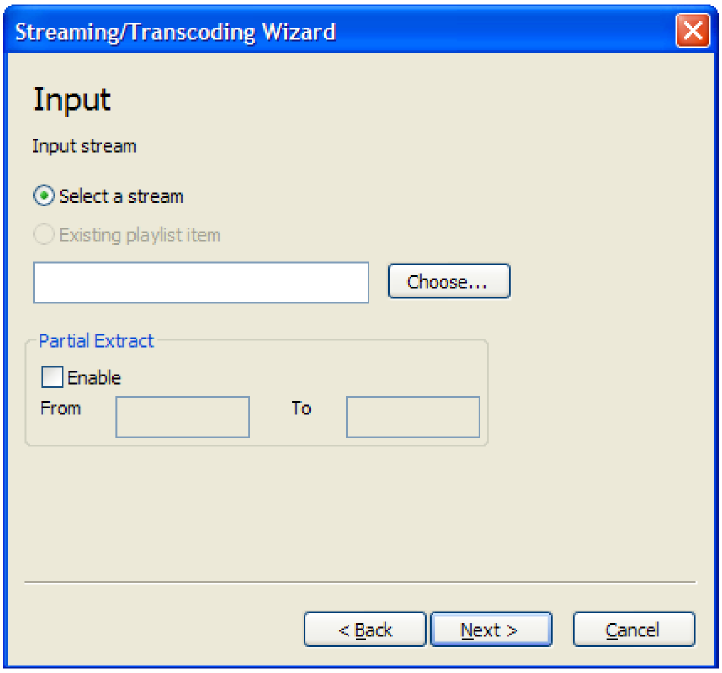


Figure 5.100 Input

3. Verify that the 'Select a stream' radio button is selected, and click 'Choose'. The following dialog box appears.

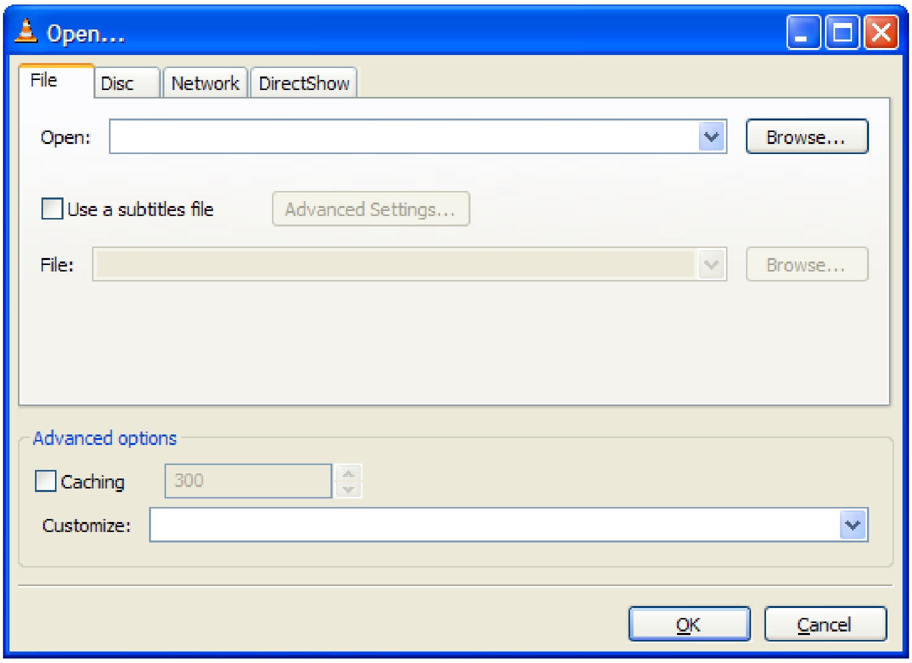


Figure 5.101 File Selection Dialog Box

4. Click 'Browse', and select the video file you would like to stream.

5. Click 'OK', and then 'Next'. The 'Streaming' screen appears.

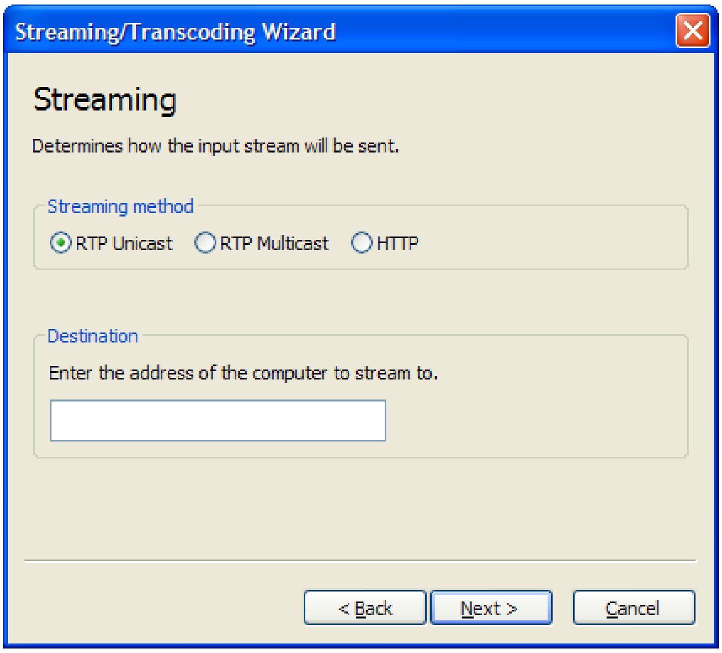


Figure 5.102 Streaming

6. Under 'Streaming method', select 'RTP Multicast'.

7. In the 'Destination' field, enter the multicast group IP address (between 224.0.0.22 – 224.0.0.102).

8. Click 'Next'. The 'Encapsulation format' screen appears.

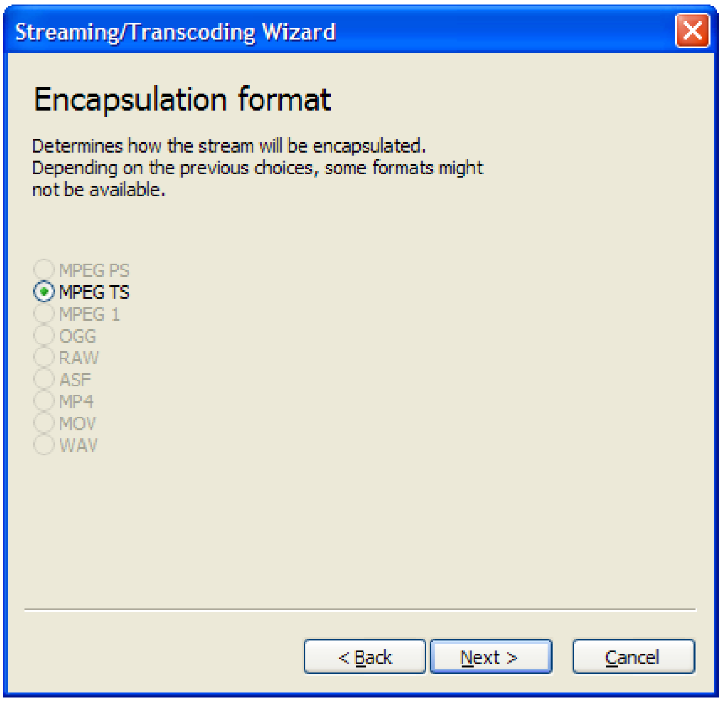


Figure 5.103 Encapsulation format

9. Verify that the 'MPEG TS' radio button is selected, and click 'Next'. The 'Additional streaming options' screen appears.

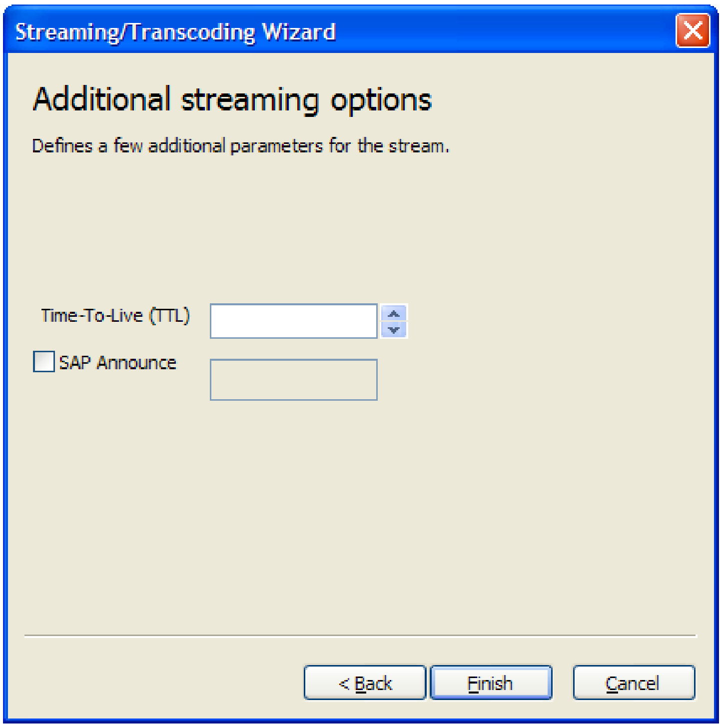


Figure 5.104 Additional streaming options

10. Set the 'Time-To-Live (TTL)' parameter to be greater than five (depends on the number of network hops).

11. Click 'Finish' to exit the wizard.

To configure the VLC client, perform the following:

1. From the 'File' menu, select 'Open Network Stream'. The following screen appears.

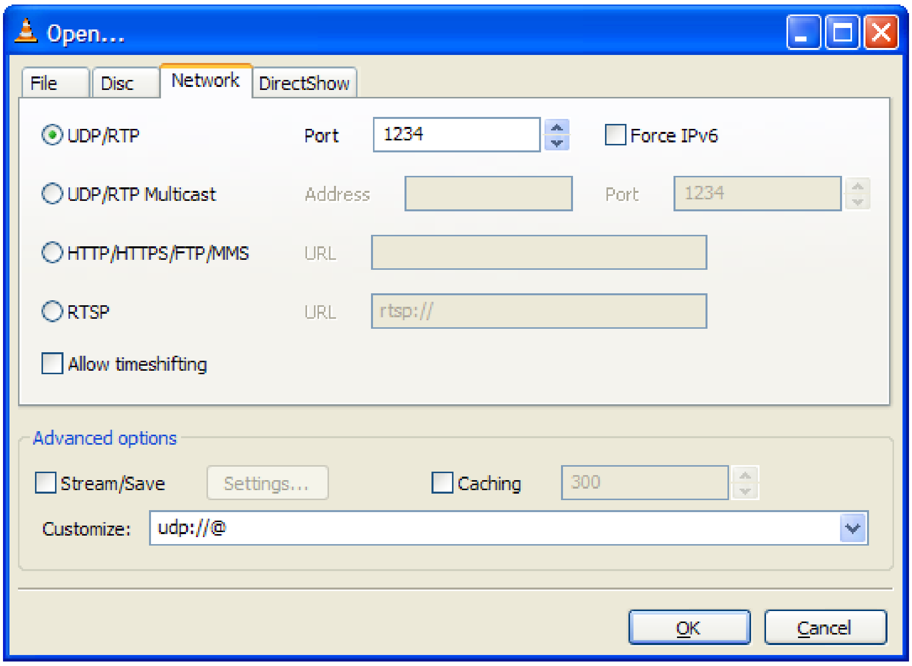


Figure 5.105 Network

2. Select the 'UDP/RTP Multicast' radio button, and enter the multicast group address (as defined in the VLC server) in the 'Address' text box that opens.

3. Click 'OK' to save the settings.

While watching the video on the LAN PC, load the network by downloading a large file from the WAN using FTP. Run the FTP's **hash** command to visualize the file download speed. The video and sound stream quality will noticeably degrade.

5.3.9.2 Using QoS for Improving the Streaming Quality

To improve the media stream quality, perform the following:

1. Designate a protocol and a specific port number for the media stream:

   a. In OpenRG's WBM, click the 'Advanced' tab and select 'Protocols'. The 'Protocols' screen appears.

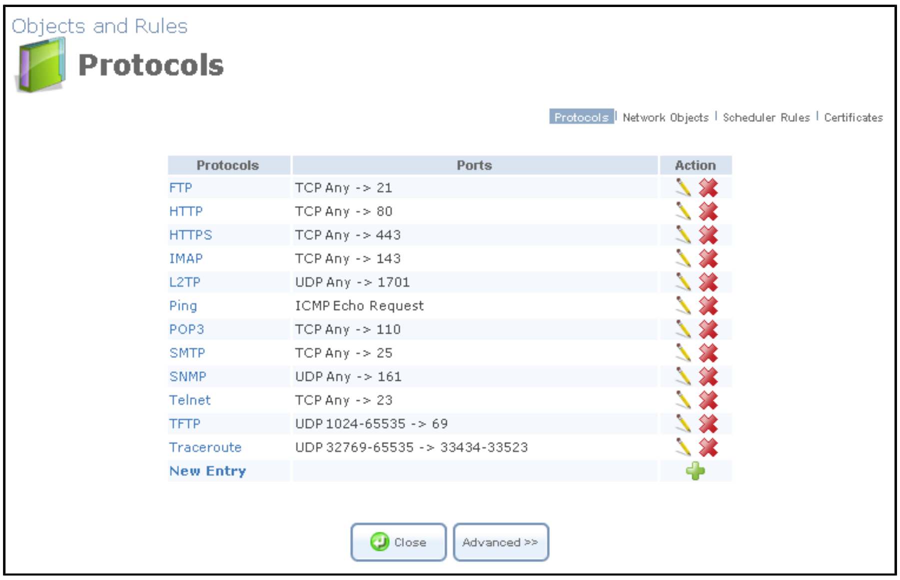


Figure 5.106 Protocols

This screen displays a list of preset and user-defined applications and common port settings. You may add new protocols to support new applications or edit existing ones according to your needs. For more information, refer to Section 6.9.1.

b. Click the 'New Entry' link. The 'Edit Service' screen appears.

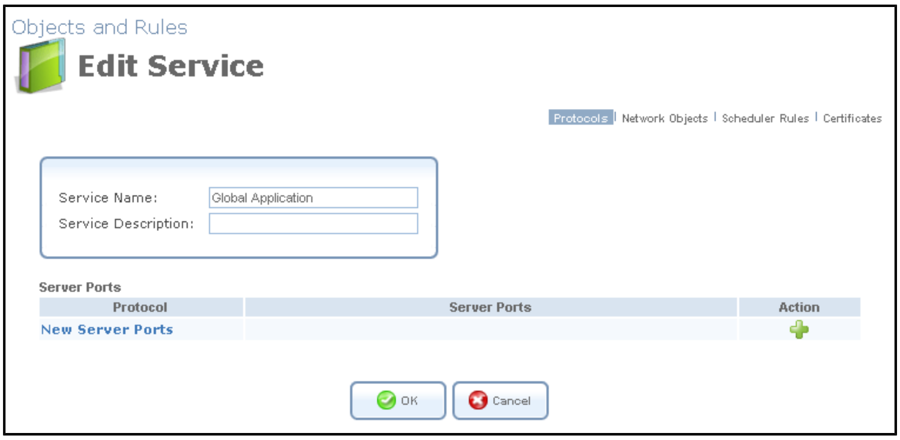


Figure 5.107 Edit Service

c. Change the default service name to 'IPTV', and click the 'New Server Ports' link. The 'Edit Service Server Ports' screen appears.

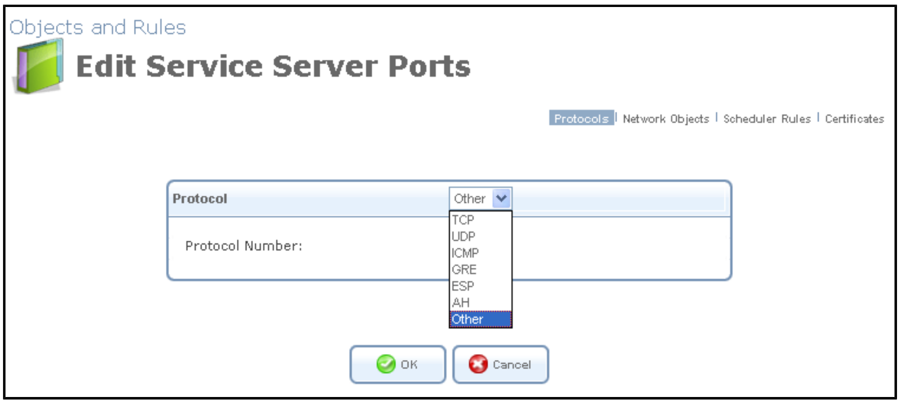


Figure 5.108 Edit Service Server Ports

d. From the 'Protocol' drop-down menu, select 'UDP'. The screen refreshes, changing to the following.

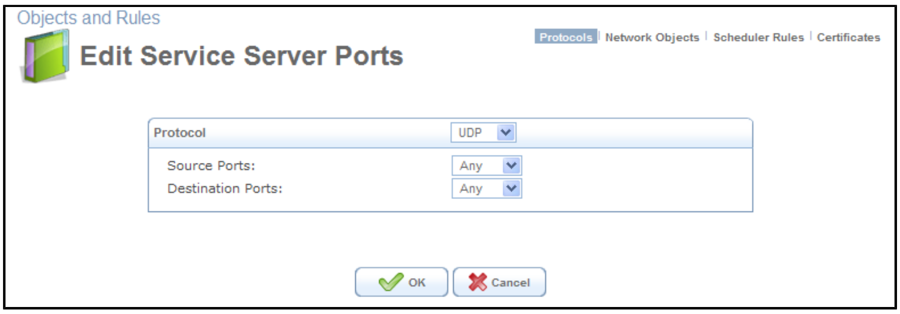


Figure 5.109 Edit Service Server Ports – UDP

e. From the 'Source Ports' drop-down menu, select 'Any'.

f. From the 'Destination Ports' drop-down menu, select 'Single' and enter port 1234 (the default port to which VLC sends the media stream).

g. Click 'OK' to save the settings.

2. Create a traffic shaping class ID:

a. Under the 'Services' tab, click the 'QoS' menu item and select 'Traffic Shaping'. The 'Traffic Shaping' screen appears, displaying the bandwidth you have set on the default WAN device.

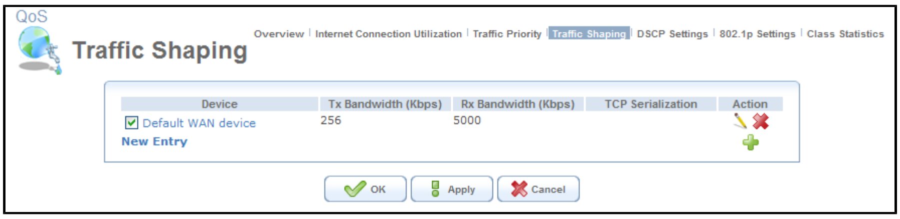


Figure 5.110 Traffic Shaping

b. Click the 'Default WAN device' link or its action icon . The 'Edit Device Traffic Shaping' screen appears.

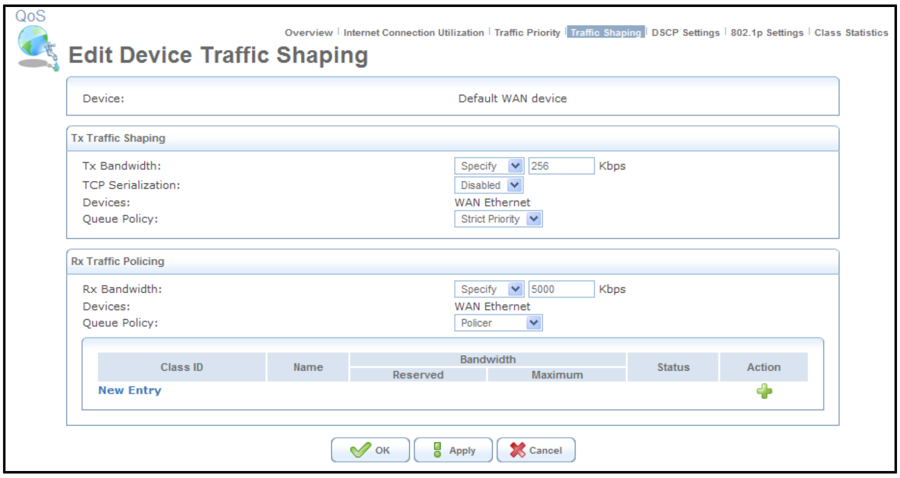


Figure 5.111 Edit Device Traffic Shaping

c. Under 'Class ID', click the 'New Entry' link. The 'Add Policing Class' screen appears.

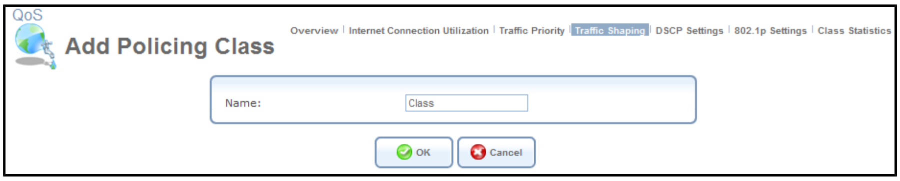


Figure 5.112 Add Policing Class

d. Change the default class name to 'IPTV', and click 'OK'. The 'Edit Device Traffic Shaping' screen appears with the IPTV class entry displayed in the 'Rx Traffic Policing' section.

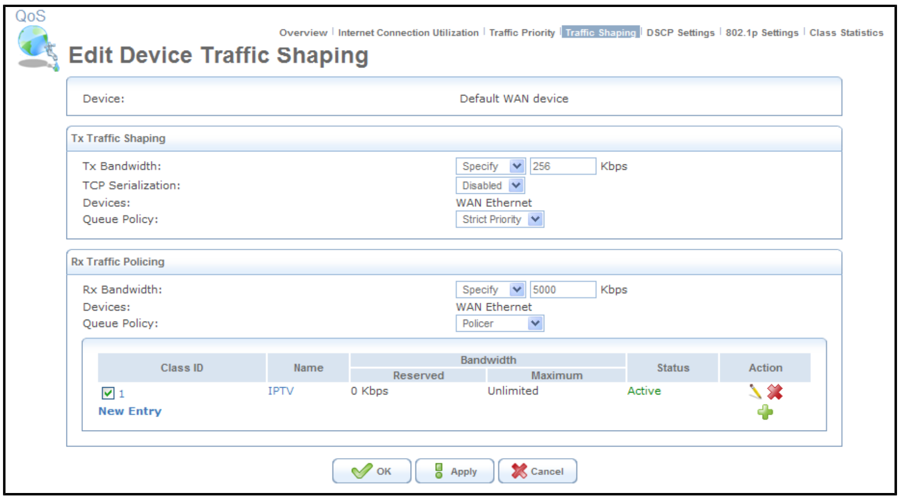


Figure 5.113 Edit Device Traffic Shaping – IPTV Class

e. Click the 'IPTV' link or its action icon . The 'Edit Policing Class' screen appears.

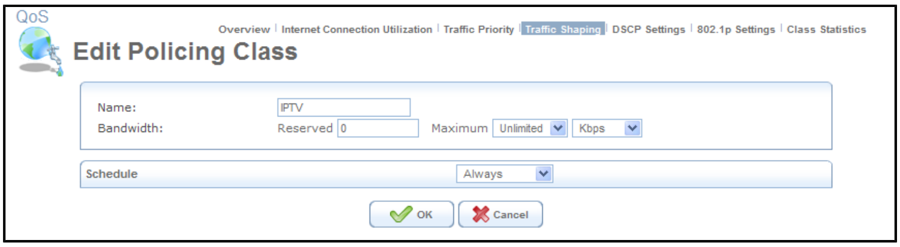


Figure 5.114 Edit Policing Class – IPTV

f. In the 'Reserved' field of the 'Bandwidth' parameter, enter 3000 and click 'OK'. You will be redirected back to the 'Edit Device Traffic Shaping' screen (see Figure 5.113). The bandwidth reserved for the IPTV will be displayed in its respective field.

3. As the last step, define a priority rule for the incoming traffic:

   a. Under the 'QoS' menu item, click 'Traffic Priority'. The corresponding screen appears.

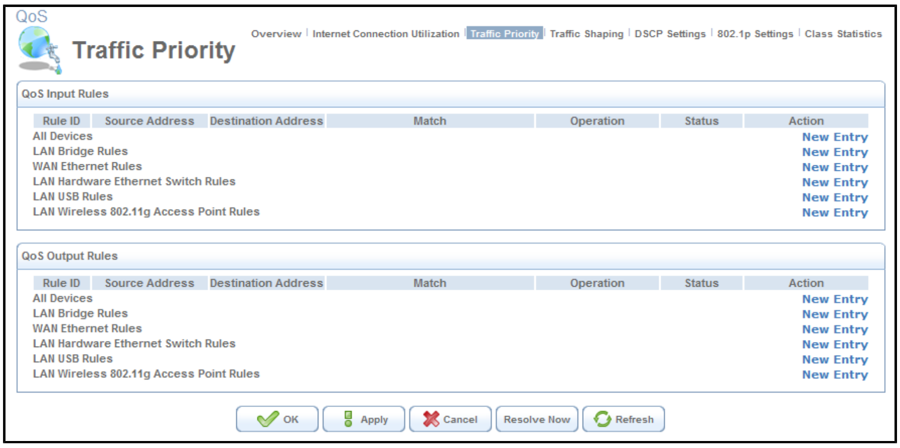


Figure 5.115 Traffic Priority

   b. In the 'Qos Input Rules' section, click the 'New Entry' link of the 'WAN Ethernet Rules' item. The 'Add Traffic Priority Rule' screen appears.

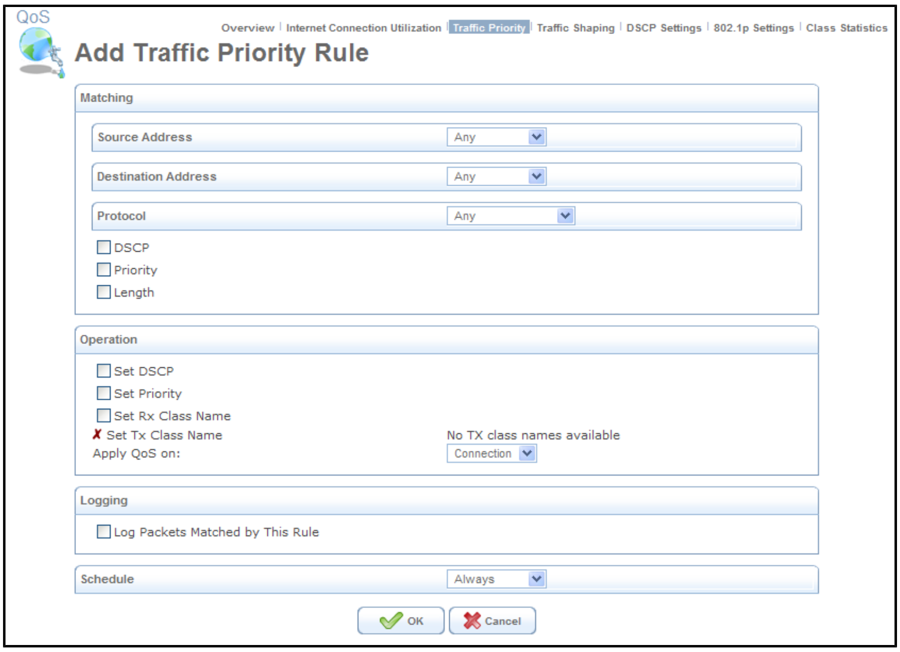


Figure 5.116 Add Traffic Priority Rule

c. From the 'Protocol' drop-down menu, select 'IPTV' (if it is not displayed, select 'Show All Services'). The screen refreshes, displaying the IPTV protocol entry.

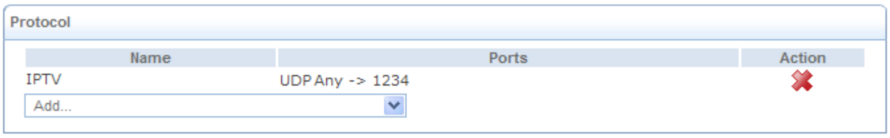


Figure 5.117 Add Traffic Priority Rule – IPTV Protocol

d. Under 'Operation', select the 'Set Rx Class Name' check box. The screen refreshes, displaying the IPTV Rx class.

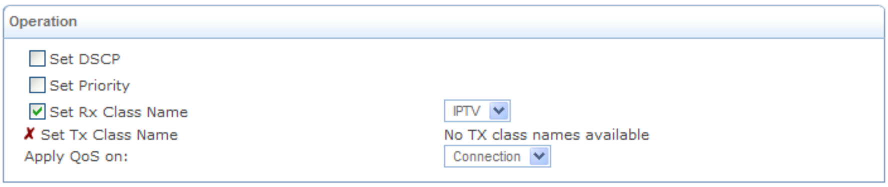


Figure 5.118 Add Traffic Priority Rule – IPTV Rx Class

e. Click 'OK' to save the settings.

Restart the video stream on the LAN while downloading a large file from the WAN using FTP. You will notice that the video stream has no disruptions, while the file download speed slows down slightly.

5.4 Sharing Your Media with the Home Network

OpenRG's Media Sharing solution enables you to share and stream media files from a storage device connected to OpenRG. You can access the shared media files with either a network-aware Consumer Electronic (CE) device, as described in Section 5.4.2, or from a LAN PC with an installed media rendering software, as described in Section 5.4.3. Both methods utilize a Universal Plug and Play (UPnP) media renderer.

5.4.1 Configuring the Media Sharing Service

Configure OpenRG's media sharing service by clicking its menu item under the 'Services' tab. The 'Media Sharing' screen appears.

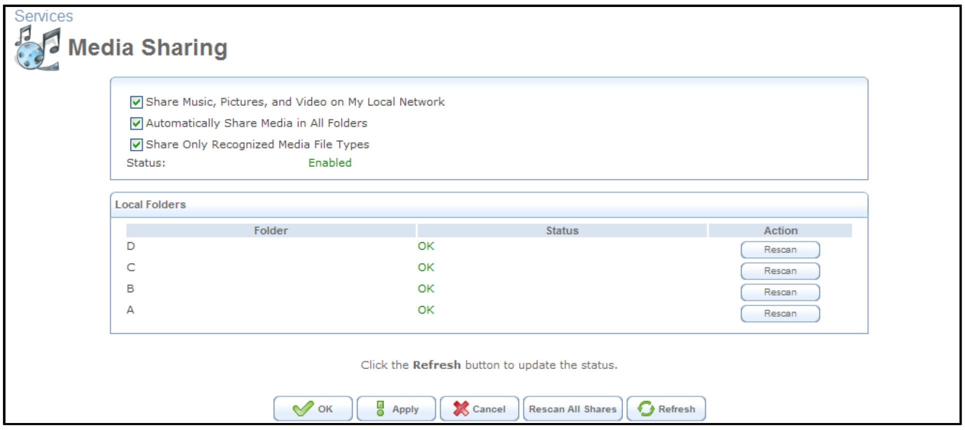


Figure 5.119 Media Sharing

The 'Media Sharing' screen contains the following options:

Share Music, Pictures and Video on My Local Network By default, this option is selected. To disable media sharing, deselect this option, and click 'Apply'.

Automatically Share Media in All Folders By default, this option is selected, causing all partitions and folders on the storage device to become shared automatically. OpenRG automatically scans the storage device for media files, and displays folders containing such files in the 'Local Folders' section of this screen. To disable the automatic sharing and manually share a specific partition or folder, perform the following:

1. Deselect the 'Automatically Share Media in All Folders' check box and click 'Apply'. The screen refreshes.

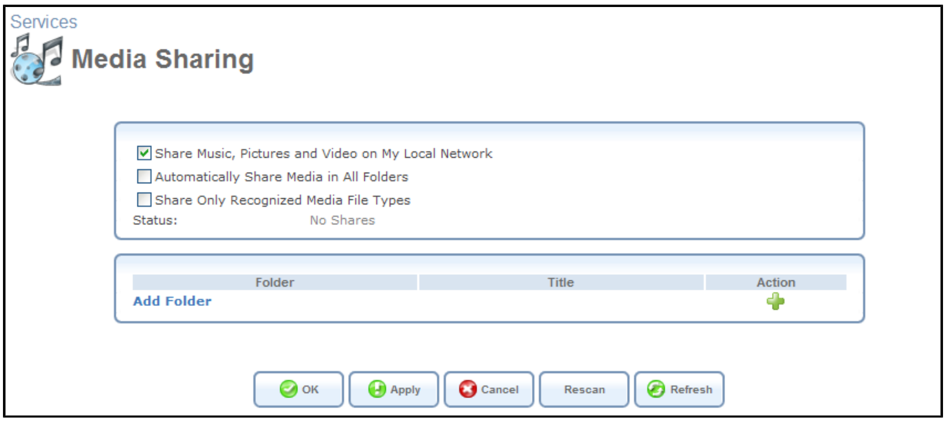


Figure 5.120 Manual Folder Sharing Mode

The 'Status' field changes to 'No Shares', and a new section appears, enabling you to create and manage a list of manually shared partitions and their folders.

2. Click the 'Add Folder' link, or the action icon . The 'Folder Settings' screen appears.

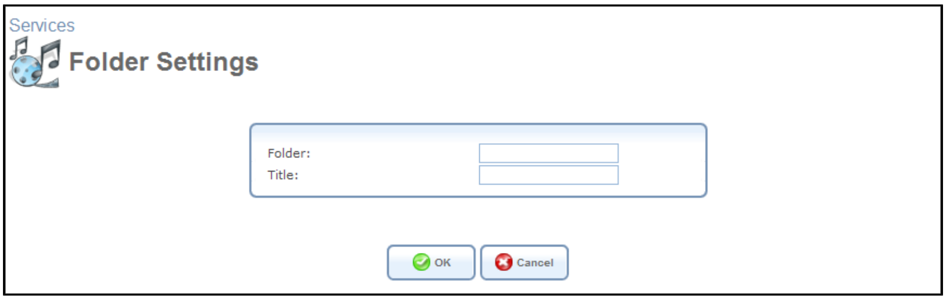


Figure 5.121 Folder Settings

3. In the 'Folder' field, enter the exact path (for example, **A/Music**, where 'A' is a partition's letter, and 'Music' is a folder on this partition).

> Note: The partition's letter cannot be changed. OpenRG automatically assigns a letter to a partition, once the storage device is connected. For more information, refer to Section 5.9.7.

4. In the 'Title' field, enter a descriptive title for the folder (for example, 'Pop Music'). Note that entering this information is mandatory.

5. Click 'OK' to save the settings. The 'Media Sharing' screen appears, displaying the shared partition. If necessary, repeat the same procedure to share additional partitions and their folders.

At any time, you can edit the partition or folder sharing settings by clicking its action icon . In addition, you can remove a partition or a folder from the shares list by clicking its action icon .

> Note: In case of changing the sharing settings, click the 'Rescan' button in the WBM's 'Media Sharing' screen before trying to access the shared media remotely. Clicking the 'Rescan' button updates the media database with the current shared media content and its path. The more disk space the media files occupy, the longer the scanning process may take.

Share Only Recognized Media File Types When this option is selected, only recognized media files are shared. Recognized media file formats include:

- Audio: MP3, OGG, WAV, and WMA.
- Video: MPEG, MPG, MPE, ASF, AVI, DIVX, WMV, MOV, and QT.
- Graphics: JPEG, JPG, JPE, GIF, PNG, TIFF, TIF, and BMP.

OpenRG adds the **MEDIASRV.DB** file to all the writable partitions it identifies on the storage device. This is an index file that the media server uses to access the media files on the disk. Therefore, do not delete this file.

When adding or removing a media file via OpenRG's file server, the media database is updated automatically. However, if other file management utilities are used (for example, FTP) to add or remove a file, click the 'Rescan' button to update the database with the changes. Otherwise, OpenRG will update the database during its periodic scanning of the shared media, which is performed once every 24 hours.

5.4.2 Streaming Your Media to a TV via a Media Client Device

OpenRG enables you to share and stream media files (music, pictures, and video) from its storage device to a TV set, over a media client device. The following sections explain how to connect this device to a TV set and the gateway, as well as how to stream the shared media content.

5.4.2.1 Connecting a Media Client

A modern media client device includes a network-aware Universal Plug and Play (UPnP) media renderer. Typically, this device has an RCA or coaxial connection to the TV set, as well as a LAN socket and/or a wireless LAN interface for connecting to the gateway.

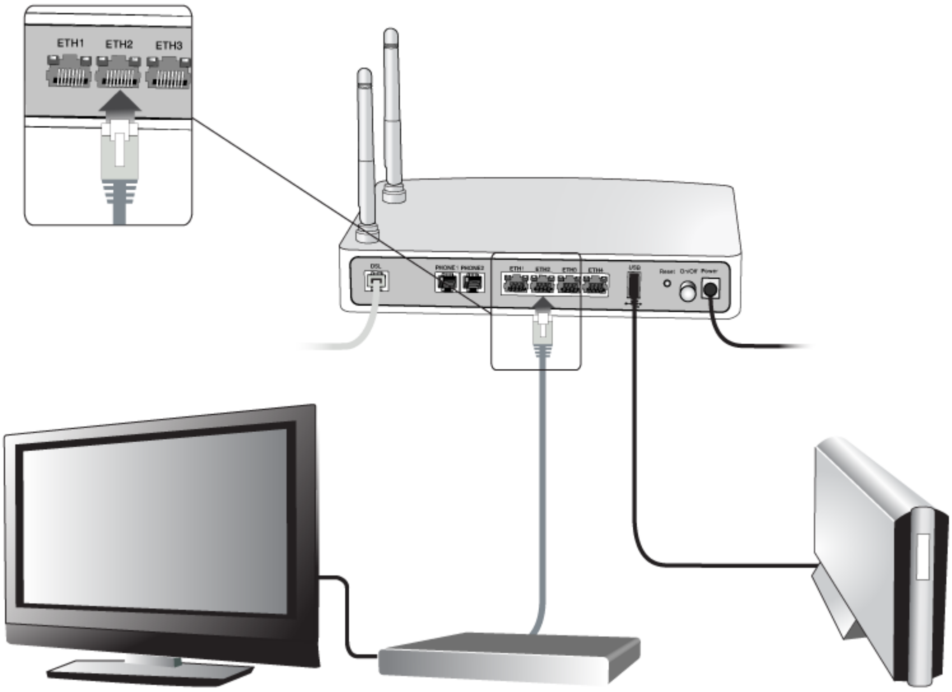


Figure 5.122 Media Client Device and Television Connection

1. Connect your TV set to the media client device according to the instructions provided with the device. Make sure you select the correct AV input on the TV set.

2. Connect the media client device to an available Ethernet port on your gateway.

> Note: If your media client device has a wireless capability, it can connect to OpenRG without cables. However, since media usage requires streaming high volumes of traffic, wireless use is recommended only if the media client device supports the 802.11n protocol.

5.4.2.2 Viewing and Streaming Media Files

Reception of OpenRG's media server broadcast by the media client device is automatic, requiring no further configuration.

1. Turn on the media client device. The following images represent the D-Link MediaLounge™ media client menu, displayed on the TV set (connected to the device).

Figure 5.123 MediaLounge Main Screen

2. Use the device's remote control to select 'My Media'. The path letter of the OpenRG share (which contains your disk content) appears.

Figure 5.124 Your Share on OpenRG

3. Select the share. The share's content is displayed.

Figure 5.125 Media Folders on a Share

> Note: MediaLounge displays the same directory hierarchies as on the storage device.

4. Select a folder, for example "photos". The folder's content is displayed.

Figure 5.126 Media Files in the Shared Folder

5. Select a photo to display.

Figure 5.127 Displaying a Photograph

In the same method, you can stream music and video files from your disk to your television.

5.4.3 Accessing the Shared Media from a LAN Computer

In this section, you will learn how to access your media content from any LAN computer, on which a media rendering client application is installed. One of such applications is **XBMC Media Center**. The following example utilizes XBMC to demonstrate how to access the shared media via a LAN computer.

After installing this application on your computer, perform the following:

1. Launch XBMC. Its main screen appears.

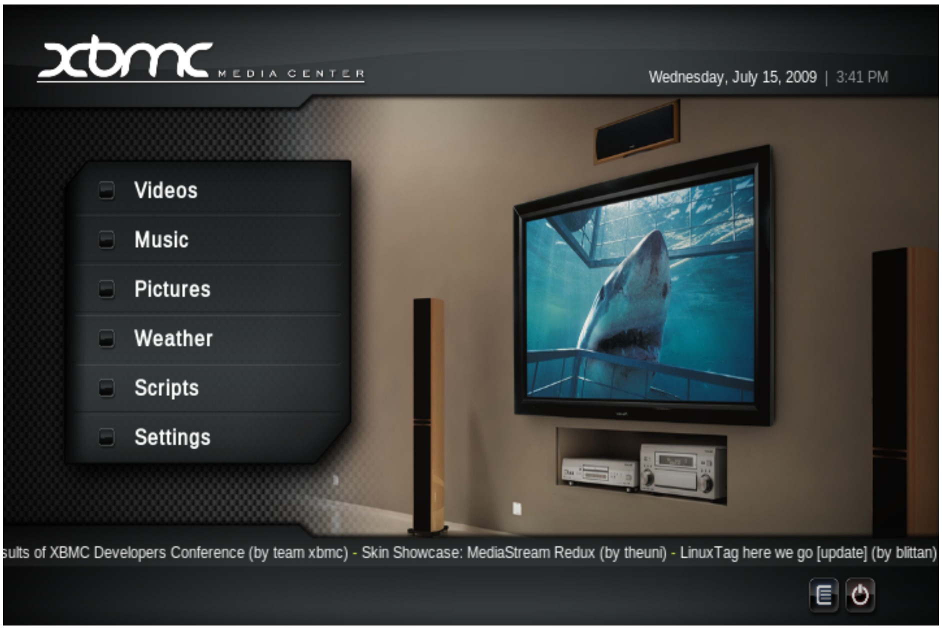


Figure 5.128 XBMC Main Screen

2. Select the type of media you would like to view by clicking the corresponding link (either 'Videos', 'Music', or 'Pictures'). For example, select 'Music'. The following screen appears.

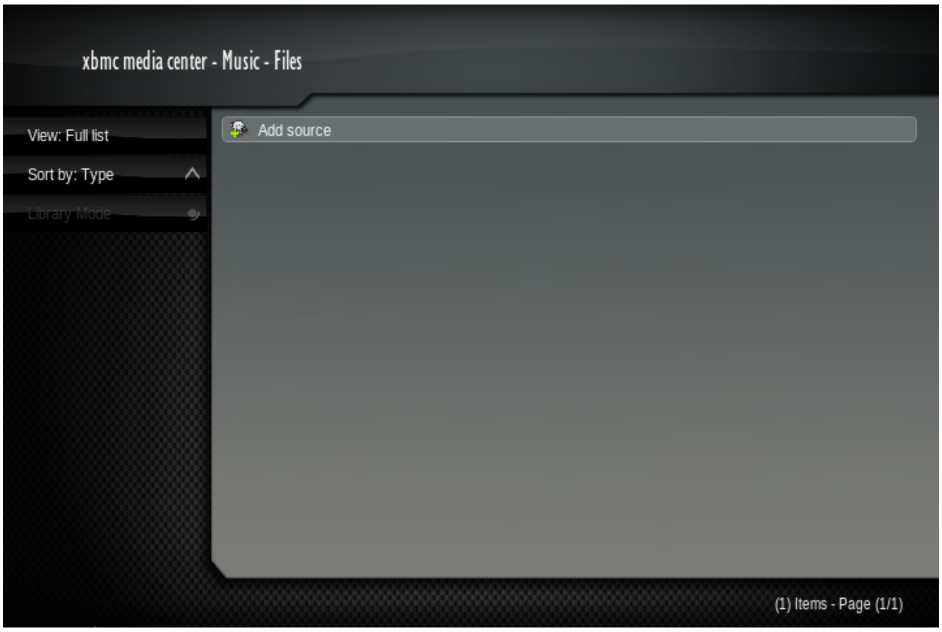


Figure 5.129 Add source

3. To obtain access to the desired media files, you must first define a path to the shared directory in which the files are stored. To do so, perform the following:

   a. Select 'Add source' (see Figure 5.129), and click the 'Browse' button in the next screen. The 'Browse for new share' dialog box appears.

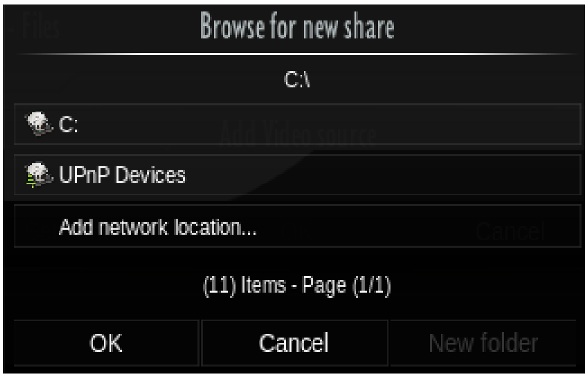


Figure 5.130 Browse for new share

b. Select the 'UPnP Devices' option. The following screen appears.

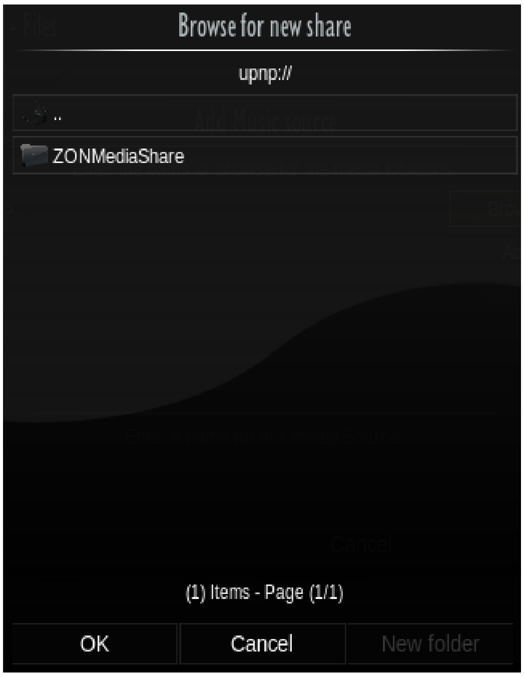


Figure 5.131 OpenRG's Media Server Link

The 'Jungo Media Server' link provides access to the storage device connected to OpenRG.

c. Click this link. After scanning your storage device for media content, XBMC displays the shared partition(s) on which it has detected media files.

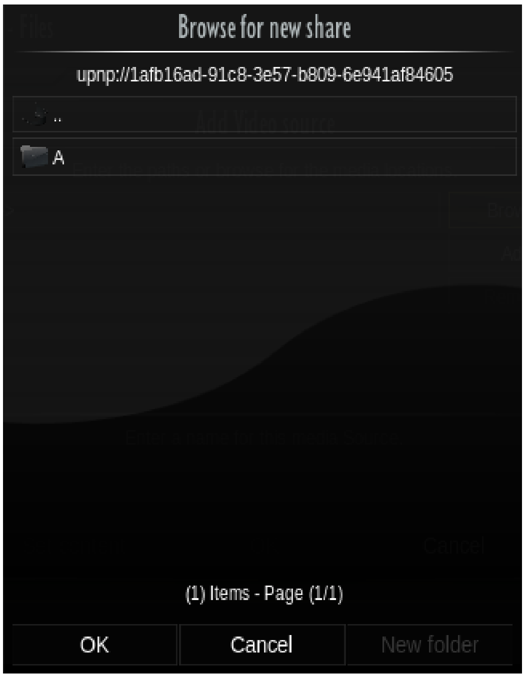


Figure 5.132 Shared Partition Containing Media Files

d. Click the partition's link. The shared media directories are displayed.

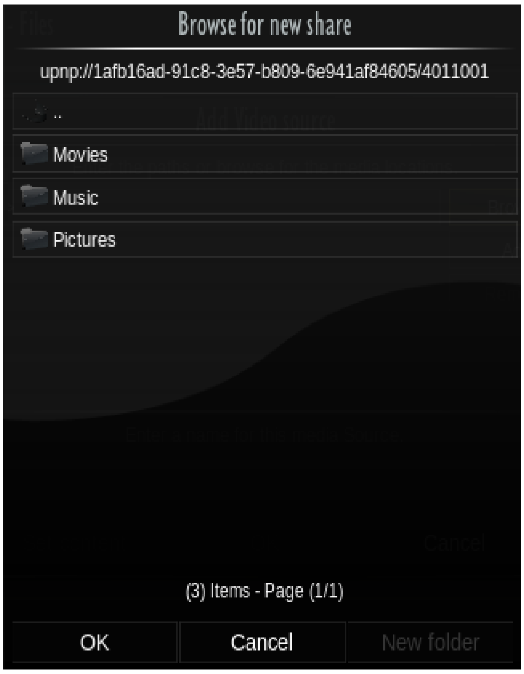


Figure 5.133 Media Directories on a Share

Note that XBMC displays the same directory hierarchies as on the storage device.

e. Select a directory in which the desired media files are located.

f. To save the path to the media directory, click 'OK' in the directory's 'Browse for new share' dialog box, and confirm in the next dialog box. This will create a shortcut

(named 'Jungo Media Server') to the selected directory, enabling you to access the shared media from XBMC.

Figure 5.134 Jungo Media Server Shortcut

4. Click the 'Jungo Media Server' shortcut. A list of media files stored in the selected directory will be displayed.

Figure 5.135 Media Files in the Shared Directory

> Note: In case the media directory specified in the path contains subdirectories, they will be displayed when clicking the 'Jungo Media Server' link. Select the desired subdirectory to display the files it contains.

5. Click a file's link to start playing it with XBMC.

Similarly, perform the above procedure to define paths for the other types of media you would like to access.

5.5 Utilizing Telephony on Your Gateway

OpenRG's Analog Telephone Adapter (ATA) Voice solution enables you to connect multiple phones over a single broadband connection, providing the benefits and quality of digital Voice Over IP (VoIP). This solution enables you to place and receive calls over the Internet using a standard telephone set connected to OpenRG.

This section assumes that you have already connected your telephone equipment to the gateway, as described in the 'Connecting a Telephone' section of the OpenRG Quick Start Guide.

OpenRG provides two types of independent telephone usages: external calling—when the gateway is provisioned with SIP telephone lines, and internal communication within the home network.

Note: OpenRG's voice functionality is based on the Asterisk VoIP stack.

5.5.1 Configuring Your Telephone Line Services

Before using your telephone, configure the services available on its line according to your preferences. In the 'Line Settings' screen under the 'Voice' menu item, click the line's action icon . In the 'Services' section, select the services you would like to activate.

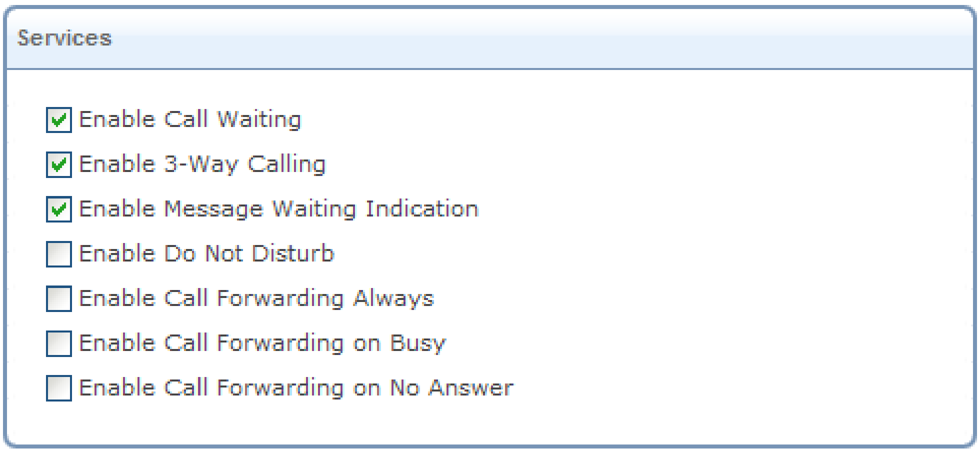


Figure 5.136 Line Settings – Services

Enable Call Waiting Select this check box to enable the Call Waiting feature.

Enable 3-Way Calling Select this check box to allow all forms of three-way conversations. When this option is disabled you will not be able to place a call on hold, transfer a call or engage in a call conference.

Enable Message Waiting Indication Select this check box to play a special stutter tone whenever you receive a voice message.

Enable Do Not Disturb Select this check box to prevent calls from reaching your line. The caller will hear a busy tone. This feature can also be enabled or disabled by dialing *78 or *79 respectively.

Enable Call Forwarding Always Select this check box to forward incoming calls to another telephone number. The screen refreshes, displaying a field for entering the alternate number.

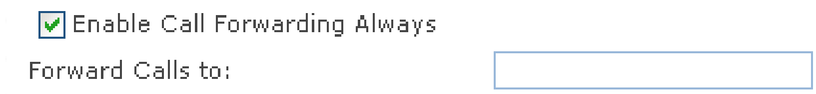


Figure 5.137 Enable Call Forwarding Always

This feature can also be enabled or disabled by dialing *72 (and the alternate number) or *73 respectively.

Enable Call Forwarding on Busy Select this check box to forward incoming calls to another telephone number when the line is busy. The screen refreshes, displaying a field for entering the alternate number.

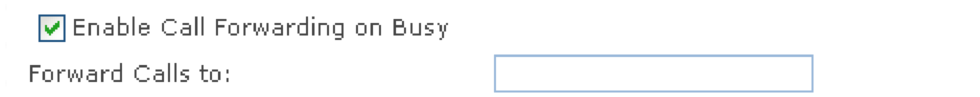


Figure 5.138 Enable Call Forwarding on Busy

This feature can also be enabled or disabled by dialing *90 (and the alternate number) or *91 respectively.

Enable Call Forwarding on No Answer Select this check box to forward incoming calls to another telephone number if the call is not answered within a specific timeframe. The screen refreshes, displaying a field for entering the alternate number, and a field for determining the timeframe to ring before the call is forwarded.

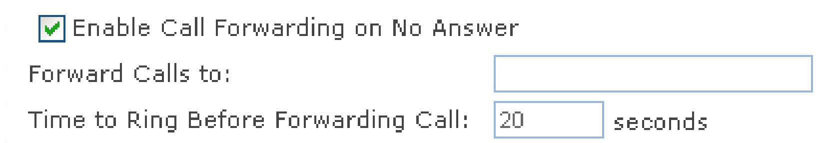


Figure 5.139 Enable Call Forwarding on No Answer

This feature can also be enabled or disabled by dialing *92 (and the alternate number) or *93 respectively.

5.5.2 Operating Your Telephone

Following are several guidelines that will help you perform basic telephne operations.

- **Placing a Call**

  1. Pick up the handset of the phone (off-hook).
  2. Dial the extension number (both '#' and the number) or the remote party's number. To have the call sent out immediately, you may dial '#'.

- **Answering a Waiting Call**
  When the Call Waiting feature is enabled, you may receive a call while engaged in another call. When such call arrives, you will hear a call waiting tone.

  1. To answer a waiting call, press 'Flash'.
  2. 'Flash' may be used to switch back and forth between calls.

- **Blind Transfer**
  To transfer an existing call (B) to a third party (C) without consultation, perform the following:

  1. Press 'Flash'. Party B will now be placed on hold, and you will hear a dial tone.
  2. Dial *98. You should hear three short beeps followed by a dial tone.
  3. Dial party C's number. You should hear a high toned beep followed by two low toned beeps, followed by a dial tone. B is now initiating a call to C. You may now dial a new call or hang up the phone.

- **Call Transfer With Consultation**
  To transfer an existing call (B) to a third party (C), perform the following:

  1. Press 'Flash' on the phone. Party B will now be placed on hold, and you will hear a dial tone.
  2. Dial party C's number or a pre-configured speed dial number followed by '#' (you can engage in conversation).
  3. To complete the transfer, place the phone's handset on-hook.

- **3-Way Conference**
  To extend an existing call (B) into a 3-way conference by bringing in an additional party (C), perform the following:

  1. Press 'Flash' on the phone. Party B will now be placed on hold and you will hear a dial tone.

2. Dial party C's number or a pre-configured speed dial number followed by '#' (you can engage in conversation).

3. Press 'Flash' to join both C and B to a single conference.

4. When you place the phone's handset on-hook, party B and party C will remain in conversation.

5.5.3 Configuring and Using Speed Dial

You can assign speed dial numbers to parties that you call frequently. Speed dial entries can be configured according to three types of destinations:

- **Proxy speed dial entry** This entry is intended for calling users that have an account with your telephone service provider.

1. Click the 'Speed Dial' link under the 'Voice' menu item. The 'Speed Dial' screen appears.

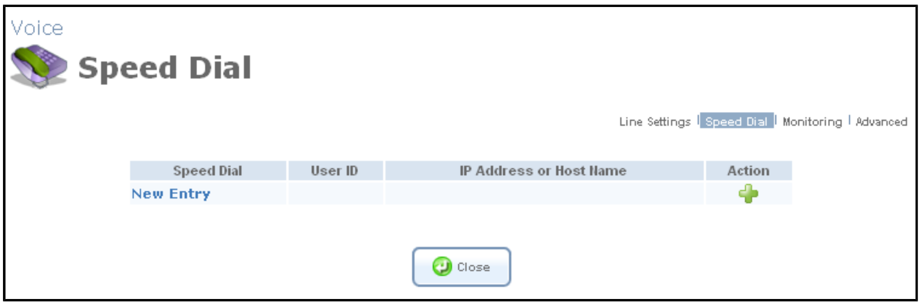


Figure 5.140 Speed Dial

2. Click the 'New Entry' link to add a new speed dial entry. The 'Speed Dial Settings' screen appears.

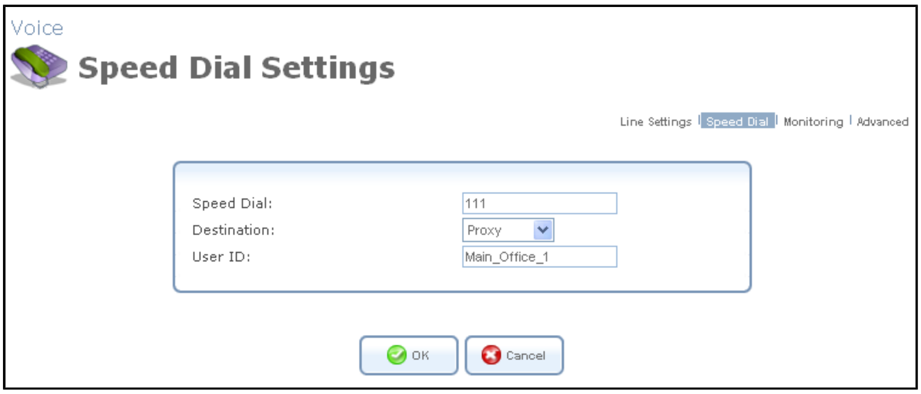


Figure 5.141 Speed Dial – via Proxy

3. Enter the following parameters:

Speed Dial A shortcut number that you will dial to call this party.

Destination The entry's destination, in this case a proxy.

User ID Specify the remote party's user ID (most commonly the telephone number).

4. Click 'OK' to save the settings.

- **Local line speed dial entry** This entry is intended for calling the other lines in your home network (local lines connected to your gateway).

1. In the 'Speed Dial' screen (see Figure 5.140), click 'New Entry' and select the 'Local Line' option from the drop-down menu. The screen refreshes.

Figure 5.142 Speed Dial - Local Line

2. Enter the following parameters:

Speed Dial A shortcut number that you will dial to call this party.

Destination The entry's destination, in this case a local line.

Line The drop-down menu displays your pre-defined local lines. Select a destination line.

3. Click 'OK' to save the settings.

- **Direct call speed dial entry** This entry is intended for calling any telephone number over the Internet.

1. In the 'Speed Dial' screen (see Figure 5.140), click 'New Entry' and select the 'Direct Call' option from the drop-down menu. The screen refreshes.

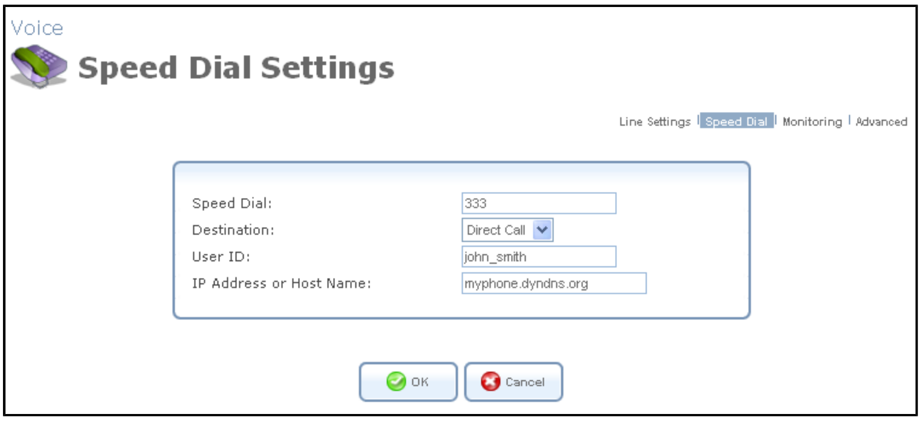


Figure 5.143 Speed Dial – Direct Call

2. Enter the following parameters:

   Speed Dial A shortcut number that you will dial to call this party.

   Destination The entry's destination, in this case a direct call.

   User ID Specify the remote party's user ID (most commonly the telephone number).

   IP Address or Host Name Specify the IP address or host name of the remote party's SIP client.

3. Click 'OK' to save the settings.

5.5.4 Sending a Fax

You can send and receive faxes over an OpenRG telephone line. Simply connect a fax machine to an active FXS telephone port on the gateway, and send the fax as you would from any other telephone.

> Note: This feature is currently available on the Broadcom 96358 platform only.

Although you can send and receive faxes with the default settings, OpenRG enables you to configure the fax transmission method and codec. In the 'Line Settings' screen under the 'Voice' menu item, click the line's action icon . In the 'Fax Transmission' section, configure the following options.

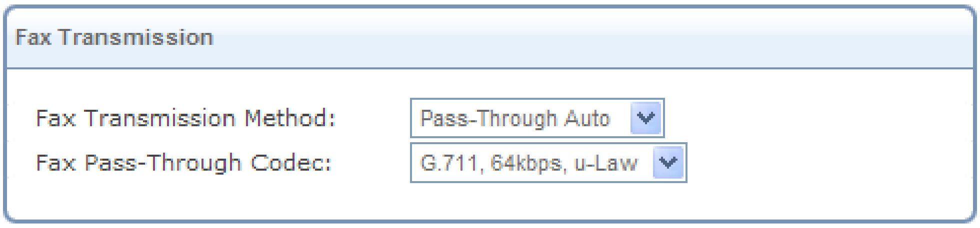


Figure 5.144 Line Settings – Fax Transmission

Fax Transmission Method The method used to switch to a codec that supports transmission of fax messages. Select a method from the drop-down menu:

- **None** Selecting this option deactivates this feature. The codec agreed upon by both sides of the conversation (refer to Section 5.5.8.6) , which does not necessarily support fax transmission, will not change. Therefore fax trasmission may fail.
- **T.38 Auto** Fax tones will be converted into T.38 packets and then transmitted. This digital mode is the most reliable fax transmission method.
- **Pass-Through Auto** A conversation will begin with the codec agreed upon by both sides. If fax tones become present, OpenRG will switch to the codec selected in the next drop-down menu, which supports fax transmission.
- **Pass-Through Force** Select this option to ensure that OpenRG begins all conversations with the fax-supporting codec selected in the next drop-down menu.

Fax Pass-Through Codec This option is only visible if a Pass-Through method is selected. Select either the u-Law or A-Law codec supporting fax transmission.

5.5.5 Customizing Your Phone Service with a Numbering Plan

A numbering plan is a set of preconfigured shortcut numbers that when dialed, perform preset actions. The caller can dynamically activate or deactivate certain actions, using the telephone keypad. For example, the caller can activate call forwarding by dialing a prefix and the number to which to forward the call.

In the 'Line Settings' screen under the 'Voice' menu item, click the line's action icon . In the 'Numbering Plan' section, configure the following options.

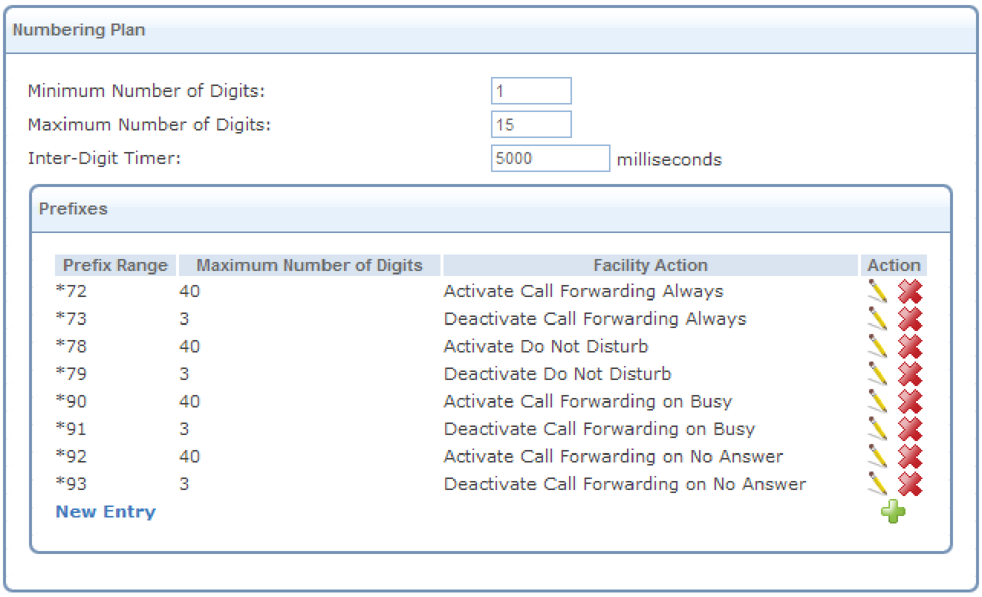


Figure 5.145 Line Settings – Numbering Plan

Minimum Number of Digits The minimum number of digits that must be dialed in order for OpenRG to send out the call.

Maximum Number of Digits The maximum number of digits that can be dialed in order for OpenRG to send out the call.

Inter-Digit Timer Specifies the duration (in milliseconds) of allowed inactivity between dialed digits. If the limit is exceeded, the dialing process times out and a warning tone is played. When you work with a proxy or gatekeeper, the number you have dialed before the dialing process has timed out is sent to the proxy/gatekeeper as the user ID to be called. This is useful for calling a remote party without creating a speed dial entry (assuming the remote party is registered with the proxy/gatekeeper).

The 'Prefixes' table displays the configured actions, containing the following parameters.

- **Prefix Range** The digits, or range of digits, constituting the prefix that activates the action. Note that a range is limited to ten digits, as only the last digit can be changed. For example, *72, 1800, 1800-1809, etc.

- **Maximum Number of Digits** The maximum number of digits that can be dialed when activating this action (including the prefix range).

- **Facility Action** The action that will be activated.

You can edit or delete the prefix entries defined in the table, using the action icons. To add a new entry, perform the following:

1. Click the 'New Entry' link. The 'Edit Prefix' screen appears.

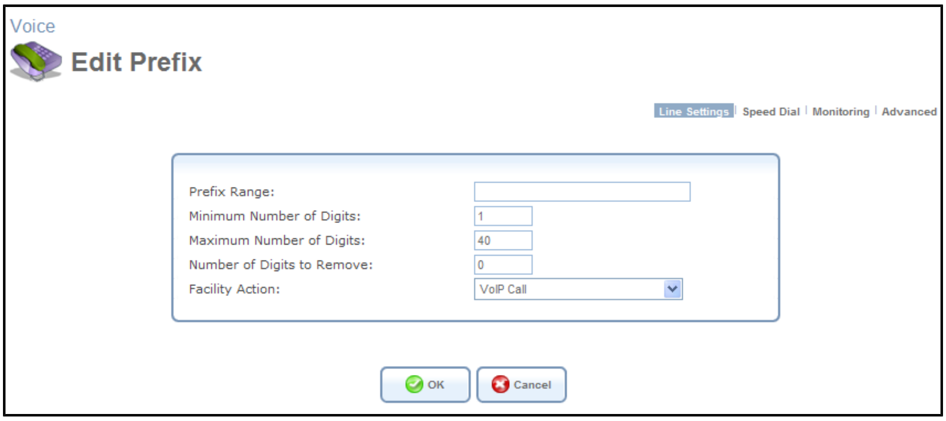


Figure 5.146 Edit Prefix

2. Enter a prefix range.

3. Determine the minimum and maximum number of digits to be dialed when activating a rule.

4. Enter the number of digits to remove from the dialed number. This is useful for removing unwanted dialed numbers, such as the digit 9 for external access.

5. Select the facility action to perform. Among activating and deactivating the "Call Forwarding" and "Do Not Disturb" features described earlier, a new "VoIP Call" action is available. Use this action to override the generic numbering plan rules. For example, if you limit callers to dial 3-digit numbers only (by setting the generic maximum number of digits to 3), but would like to enable them to dial 1-800 numbers, enter "1800" as the prefix range, and specify the maximum number of digits that 1-800 numbers may have.

6. Click 'OK' to save the settings.

5.5.6 Using Distinctive Ring

If your gateway's Digital Signal Processing (DSP) module supports the Distinctive Ring service (available on some SIP servers), you can enrich your telephone line functionality by:

- Creating additional numbers for your line, and assigning a distinctive ring pattern to each of them. This is useful, for example, if you want to distinguish between incoming calls.
- Assigning a distinctive ring pattern to the incoming calls, by matching the caller ID to a specific ring tone. By doing so, you can recognize the caller's identity before answering the call.

> Note: The availability of the service implementations depends on the SIP service provider.

To activate the Distinctive Ring service, you must first create a SIP account on a server that supports this feature. Examples of such SIP servers are Broadsoft (http://www.broadsoft.com) and Broadvoice (http://www.broadvoice.com). After registering and configuring your SIP account, enter the SIP account settings and the proxy parameters in OpenRG's 'Line Settings' screen, as described in the 'Connecting a Telephone' section of the OpenRG Quick Start Guide.

5.5.7 Ensuring Constant Connectivity with Failover

Normally, telephones connected to the FXS ports are provided with lines by a SIP service over the Internet. If your gateway also includes an *FXO* port, you can connect it to your telephone wall outlet (PSTN). In case your gateway's connection to the SIP service is disrupted, your phones can be automatically switched to the FXO port connected to the PSTN line, thereby ensuring that you always have telephone connectivity. This capability is called PSTN Failover.

> Note: This feature is currently available only on the Broadcom 96358 platform.

You can both send and receive PSTN phone calls via FXO. When a call arrives from PSTN, all telephones connected to the FXS ports will ring simultaneously, unless the 'Do Not Disturb' feature is enabled on some of them. When using an FXS line on which call waiting is enabled, you will hear a call waiting tone whenever a call arrives from PSTN.

Connect your gateway's FXO port to the telephone wall outlet. In the 'Line Settings' screen under the 'Voice' menu item, click the line's action icon . In the 'PSTN Failover' section of the external line settings screen, define under which circumstances the line failover will occur, by selecting the corresponding check boxes.

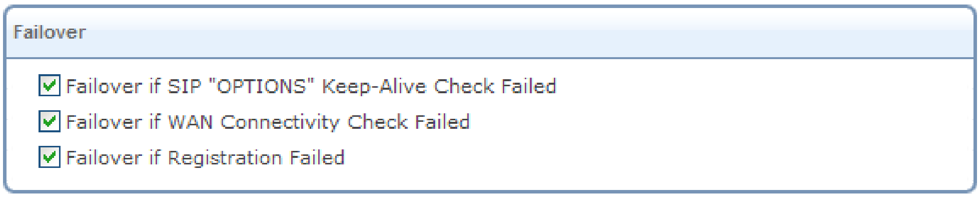


Figure 5.147 Line Settings – PSTN Failover

Failover if SIP "OPTIONS" Keep-Alive Check Failed Select this check box to enable the line failover in case the SIP server stops responding to keep-alive messages sent by OpenRG's PBX.

Failover if WAN Connectivity Check Failed Select this check box to enable the line failover in case OpenRG has detected that there is no WAN connectivity.

Failover if Registration Failed Select this check box to enable the line failover in case the line's registration on the SIP server has failed.

5.5.8 Advanced Telephony Options

This section provides advanced options intended for a technician or a system administrator.

5.5.8.1 Determining DTMF Tones

DTMFs are the tones generated by your telephone's keypad, which are used by different telephone servers (for example, for selecting an option from a menu). If required, you can change the transmission method of these tones. In the 'Line Settings' screen under the 'Voice' menu item, click the line's action icon . In the 'Advanced SIP Settings' section, configure the following options.

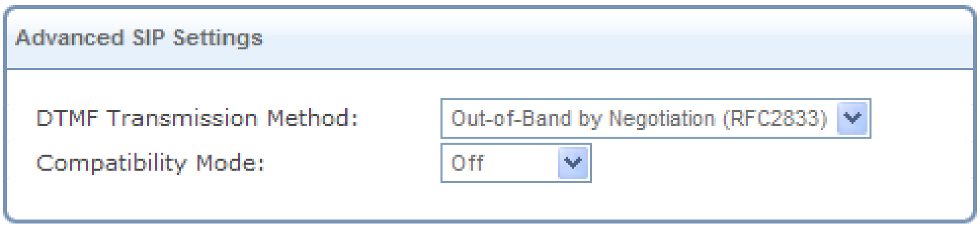


Figure 5.148 Line Settings – Advanced SIP Settings

DTMF Transmission Method Select a transmission method from the drop-down menu:

- **Inband** The DTMF keypad tones are sent within the voice stream.
- **Out-of-Band Always (RFC2833)** The DTMF keypad tones are represented by the keypad number and are sent as separate packets. This is a more reliable transmission method.

- **Q.931 Keypad** The DTMF keypad tones are sent using Q.931 messages.
- **H.245 Alphanumeric** The DTMF keypad tones are sent using an H.245 alphanumeric Information Element (IE).
- **H.245 Signal** The DTMF keypad tones are sent using an H.245 signal IE.
- **Out-of-Band by Negotiation (RFC2833)** This method allows negotiation with the remote party. DTMF tones will be sent either in-band or out-of-band, depending on the remote party's preference.
- **SIP INFO** A special SIP message that includes the DTMF event description.

Compatibility Mode If you are using Broadsoft as your SIP provider, select its mode from this drop-down menu. Otherwise, leave as "Off".

5.5.8.2 Monitoring Your Lines

You can monitor the status of your telephone lines in one convenient place—the 'Monitoring' screen. Access this screen by clicking the 'Monitoring' link under the 'Voice' menu item.

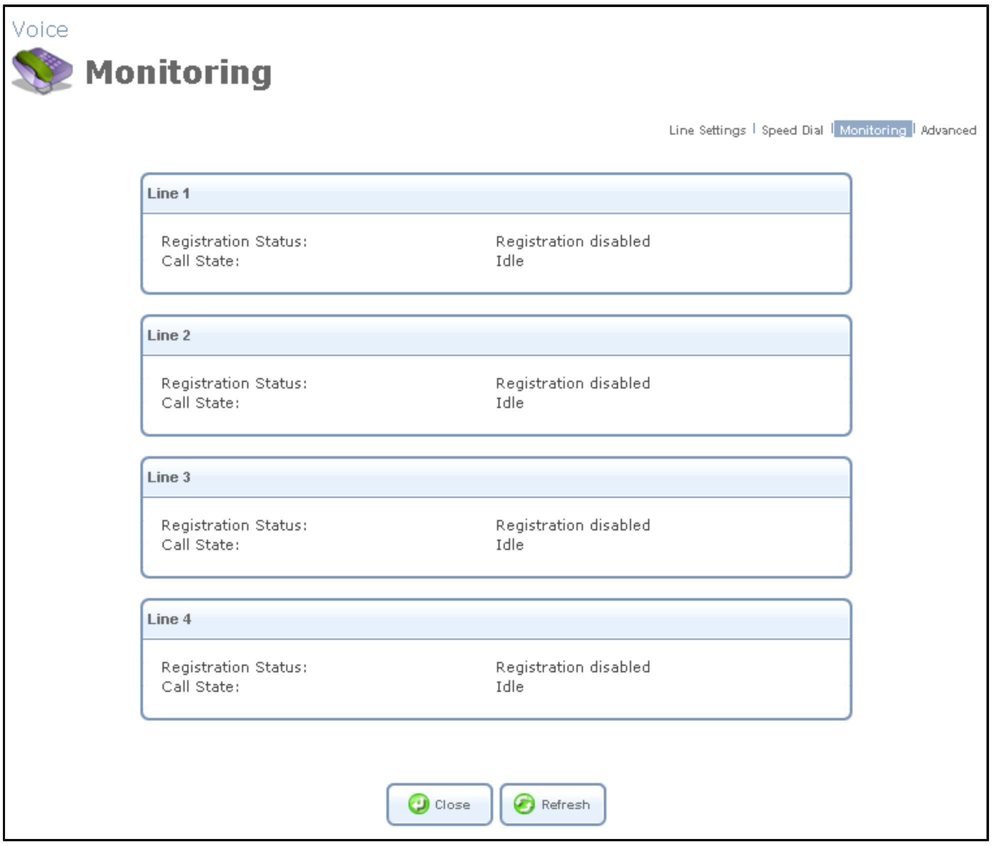


Figure 5.149 Monitoring

This screen displays all available lines and information on their statuses in real-time. These statuses include:

Registration Status Indicates whether the line is registered with a telephony service.

Call State The current state of the line—either "Idle" or "In call".
When a call is in progress, additional call statistics appear, such as the number of packets sent/received/lost, interarrival jitter, and more.

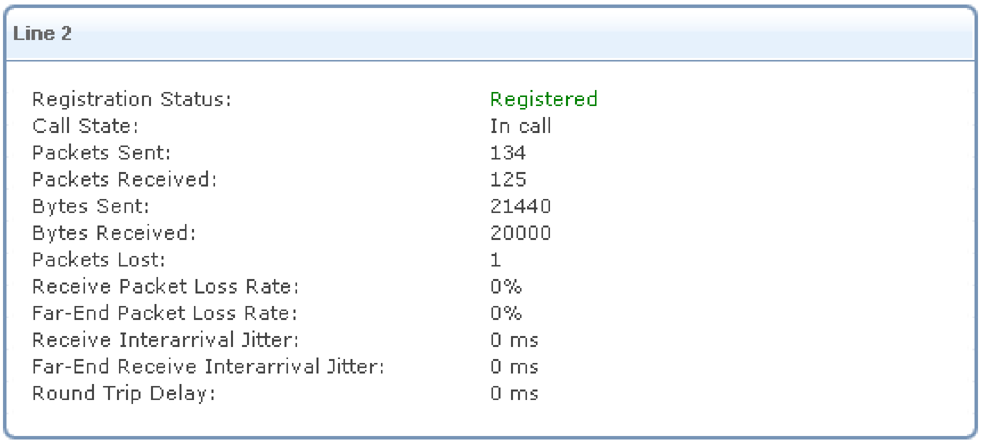


Figure 5.150 Call Statistics

5.5.8.3 Changing the Signaling Protocol

The signaling protocols available with OpenRG are Session Initiation Protocol (SIP), H.323, and Radvision's MGCP. To change your signaling protocol according to your telephone service provider, click the 'Advanced' link under the 'Voice' menu item. In the 'Signaling Protocol' section, select a protocol in the drop-down menu. A different subset of parameters will become visible with each signaling protocol choice. To apply the protocol change you must click 'Apply' (at the bottom of the 'Advanced' screen).

5.5.8.3.1 SIP

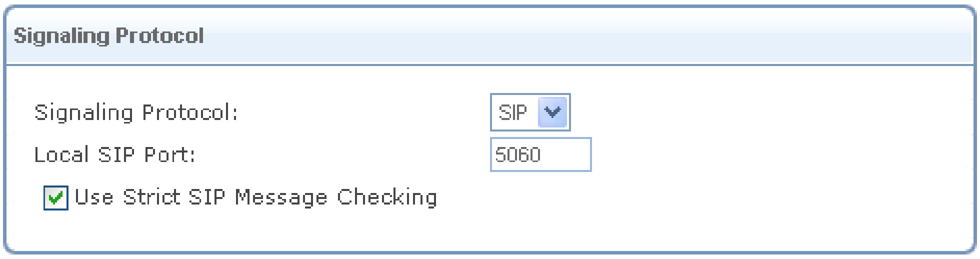


Figure 5.151 SIP Signaling Protocol

Local SIP Port The port on OpenRG that listens to SIP requests from the proxy. By default, port 5060 is used for SIP signaling of phones connected to the gateway. A common problem occurs when using a SIP agent on the LAN (for example, an IP phone). A SIP agent requires port forwarding configuration (refer to Section 5.2.3), which uses the same port—5060. This multiple use of the port causes failure of either or both services. Therefore, when configuring port forwarding for a SIP agent, you must change OpenRG's SIP port value (for example, to 5062). Note that the calling party must be made aware of this value when initiating a direct call (not using a proxy).

Use Strict SIP Message Checking By default, OpenRG uses strict SIP message checking, which includes checking of tags in headers, international character conversions in URIs, and multiline formatted headers. There are cases in which this option should be disabled to ensure interoperability with certain service providers or third party user agents (SIP endpoints).

5.5.8.3.2 H.323

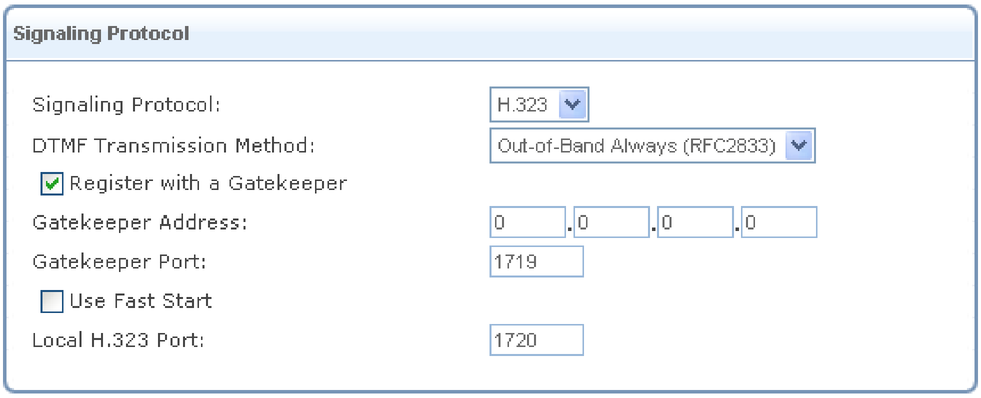


Figure 5.152 H.323 Signaling Protocol

DTMF Transmission Method Select a DTMF transmission method. For more information, refer to Section 5.5.8.1.

Register with a Gatekeeper Register the user with a gatekeeper, allowing other parties to call the user through the gatekeeper. When this item is checked, the following fields become visible:

> **Gatekeeper Address** The IP address or name of the primary gatekeeper.
>
> **Gatekeeper Port** The port on which the primary gatekeeper is listening for connections.
>
> **Specify Gatekeeper ID** Select whether a gatekeeper ID should be used for the primary H.323 gatekeeper.
>
> > **Gatekeeper ID** The identifier for the primary H.323 gatekeeper.
>
> **Registration Time to Live** Specify the valid duration of the H.323 gatekeeper registration in seconds.
>
> **Use Alternate Gatekeeper** Select this check-box to configure an alternate gatekeeper for redundancy. When this item is checked, the following fields become visible:
>
> > **Alternate Gatekeeper Address** The IP address or name of the alternate gatekeeper.
> >
> > **Alternate Gatekeeper Port** The port on which the alternate gatekeeper is listening for connections.

Use Fast Start The fast start connection method can result in quicker connection establishment, depending on the remote party's settings. Note that Microsoft NetMeeting does

not support this option, so in order to interoperate with Microsoft NetMeeting, you should disable the feature.

Use H.245 Tunneling Indicates whether H.245 packets should be encapsulated within H.225 packets.

Local H.323 Port Specify the port number to use for H.323 signaling.

The Asterisk protocol has several limitations:

1. When a gatekeeper is configured, all calls are routed through it. This has the following effect on the speed-dials:
   - Destination type "Proxy" works normally – the call is sent to the gatekeeper.
   - Destination type "Local line" – the call will succeed, however it will not be a local call. It will be routed through the gatekeeper, and will go on normally since all of the local lines are registered with this gatekeeper.
   - Destination type "Direct Call" – speed dials of this type become disabled. This will be indicated in the speed dial table. For direct call speed dials, the "IP Address or Host Name" column will include, in addition to the address, the following red remark: "Disabled in H.323 gatekeeper mode".
2. When a gatekeeper is not configured, the only way to make a non-local call is to define a "direct call" speed dial, stating the destination's IP address (or host name). Speed dials of type "Proxy" are meaningless.

5.5.8.3.3 MGCP

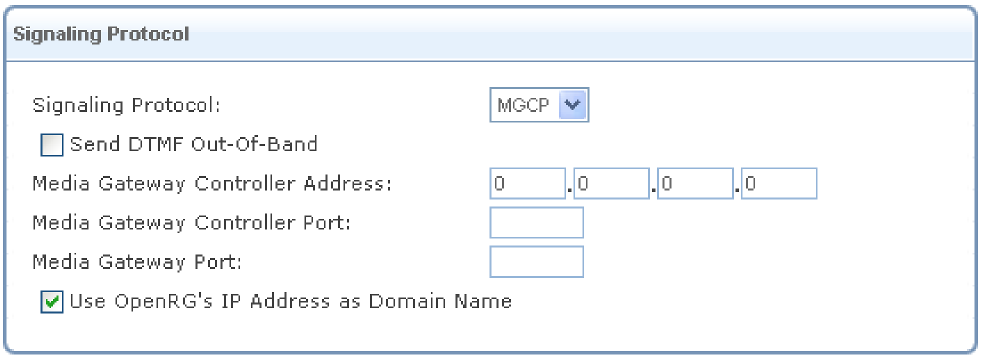


Figure 5.153 MGCP Signaling Protocol

Send DTMF Out-of-Band Select this option to use out-of-band DTMF transmission method (for more information, refer to Section 5.5.8.1).

Media Gateway Controller Address The IP address of the MGC (MGCP server), in dotted number notation.

Media Gateway Controller Port The port MGC uses to listen for connections.

Media Gateway Port The port the gateway uses for MGCP connections.

Use OpenRG's IP Address as Domain Name OpenRG's IP address will be used as the domain name for identification. Unselect this check box when provided with a domain name from the MGCP service provider. The screen will refresh, adding the following field.

Media Gateway Domain Name Enter the domain name provided by the MGCP service provider.

5.5.8.4 Changing the Reserved RTP Port Range

The voice stream is transmitted in Real Time Protocol (RTP) packets, which require a range of open ports. If the default ports are required for another application, you can enter a different start port, thus creating a new range. To change the start port, configure the following option in the 'RTP' section.

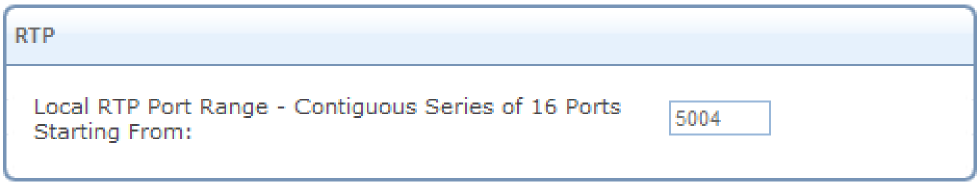


Figure 5.154 Advanced – RTP

Local RTP Port Range The range of ports reserved for Real Time Protocol (RTP) voice transport.

5.5.8.5 Configuring Quality of Service Parameters

Quality of Service (QoS) is aimed at improving the quality of voice traffic. To configure the QoS parameters, click the 'Advanced' link under the 'Voice' menu item. In the 'Quality of Service' section, configure the following options.

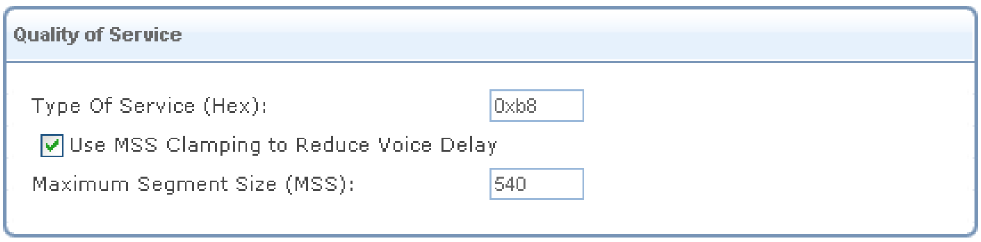


Figure 5.155 Advanced – Quality of Service

Type of Service (HEX) This is a part of the IP header that defines the type of routing service to be used to tag outgoing voice packets originated from OpenRG. It is used to tell routers along the way that this packet should get specific QoS. Leave this value as 0XB8 (default) if you are unfamiliar with the Differentiated Services IP protocol parameter.

Use MSS Clamping to Reduce Voice Delay When using Maximum Segment Size (MSS) Clamping, TCP streams routed via OpenRG when a voice call is active, will have a smaller segment size. This will cause RTP to receive better priority, and will help prevent high voice

jitter that is caused by slow upstream transmission rate, which is common with most WAN connections (DSL, DOCSIS, etc.). When checking this option, the 'Maximum Segment Size (MSS)' field appears, where you can change the maximal segment size.

5.5.8.6 Selecting Audio Codecs

Audio codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For example, G.723 is a codec that uses compression, so it is good for use where bandwidth is limited but its voice quality is not as good compared to other codecs such as the G.711.

To select the audio codecs, click the 'Advanced' link under the 'Voice' item menu. In the 'Codecs' section, configure the following options.

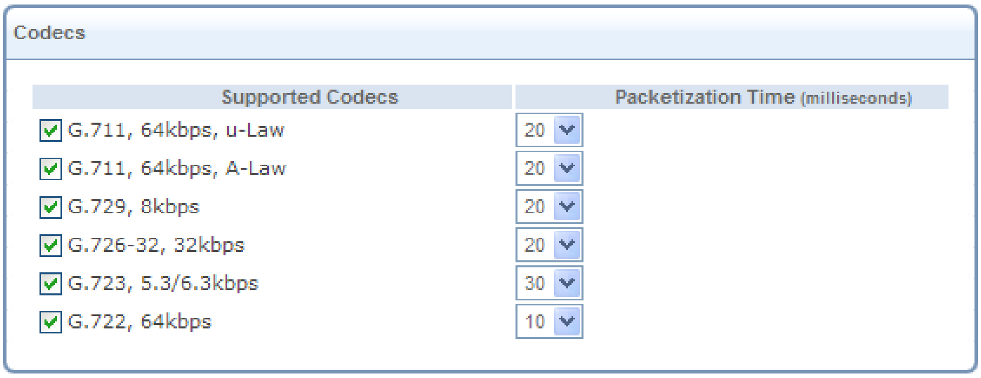


Figure 5.156 Advanced – Codecs

Supported Codecs In order to make a call, at lease one codec must be enabled. Moreover, all codecs may be enabled for best performance. When you start a call to a remote party, your available codecs are compared against the remote party's, to determine which codec will be used. The priority by which the codecs are compared is according to the descending order of their list, as depicted in the figure above. If there is no codec that both parties have made available, the call attempt will fail. Note that if more than one codec is common to both parties, you cannot force which of the common codecs that were found will be used by the remote party's client. If you do wish to force the use of a specific codec, leave only that codec checked.

Packetization Time The Packetization Time is the length of the digital voice segment that each packet holds. The default is 20 millisecond packets. Selecting 10 millisecond packets enhances the voice quality, as less information is lost due to packet loss, but doubles the load on the network traffic.

5.5.8.7 Improving Voice Reception with Echo Cancellation

Echo cancellation is the elimination of reflected signals (echoes) made noticeable by delay in the network. This also improves the bandwidth of the line. When the delay of a voice call exceeds acceptable limits, OpenRG will protect the far end from receiving any echo generated at the local end and sent back through the network.

Note: This feature is currently available on the following platforms: Intel IXP425, Broadcom BCM96358, and on platforms with the VINETIC chipset.

To improve voice reception with echo cancellation, click the 'Advanced' link under the 'Voice' item menu. In the 'Echo Cancellation' section, configure the following options.

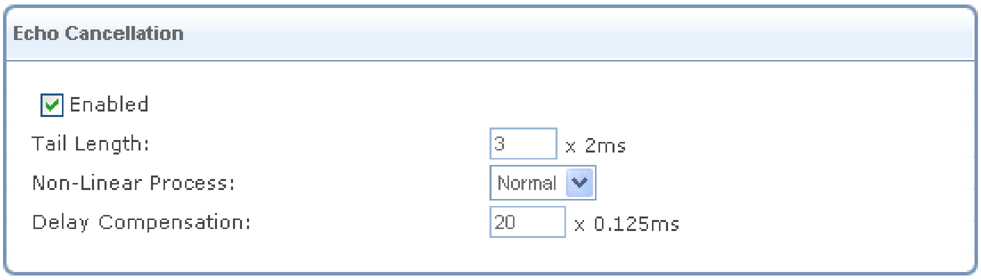


Figure 5.157 Advanced – Echo Cancellation

Enabled Select or deselect this check box to enable or disable this feature.

Tail Length Defines the length of the elapsed time frame used for calculating the extrapolation of the echo cancellation. A long tail improves the echo cancellation, but increases the load on the Digital Signal Processor (DSP).

Non-Linear Process (NLP) Determines the type of calculation that is used for removing the echo effect. You can set this feature to Normal, High or Off. Using high NLP improves the echo cancellation, but increases the load on the DSP.

Delay Compensation A time delay compensating the echo cancellation.

Note: On some platforms, the feature's graphic interface may differ from the one presented in the above figure.

5.5.8.8 Saving Bandwidth with Silence Suppression

Silence suppression enables optimization when no speech is detected. With this feature enabled, OpenRG is able to detect the absence of audio and conserve bandwidth by preventing the transmission of "silent packets" over the network.

To save bandwidth with silence suppression, click the 'Advanced' link under the 'Voice' item menu. In the 'Silence Suppression' section, configure the following options.

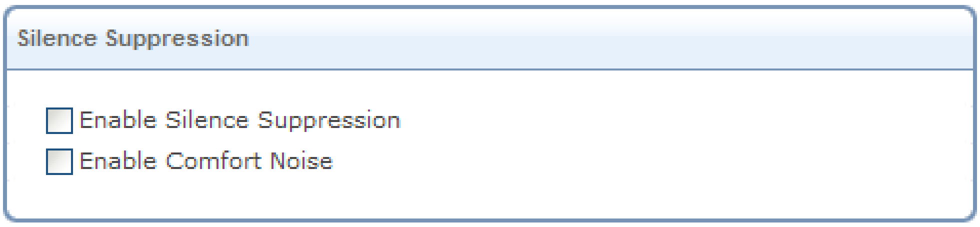


Figure 5.158 Advanced – Silence Suppression

Enable Silence Suppression Select this check box to enable this feature.

Enable Comfort Noise Select this option to play a soft "comfort" noise if the other side is performing silence suppression, in order to signal your caller that the conversation is still active.

5.5.8.9 Avoiding Voice Distortion with Jitter Buffer

A Jitter Buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly spaced intervals. Variations in packet arrival time, called "jitter", can occur because of network congestion, timing drift, or route changes. The jitter buffer intentionally delays the arriving packets so that the end user experiences a clear connection with very little voice distortion.

To avoid voice distortion with jitter buffer, click the 'Advanced' link under the 'Voice' item menu. In the 'Jitter Buffer' section, configure the following options.

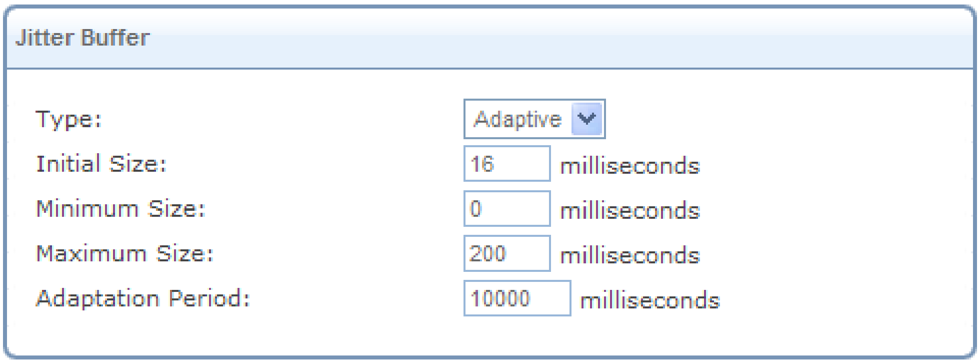


Figure 5.159 Advanced – Jitter Buffer

Type The type of the jitter buffer. Can be either adaptive or fixed. In case of adaptive jitter buffer, the following fields are visible:

Adapt According to Determines whether the jitter buffer size depends on the packet length or on the estimated network jitter.

Scaling Factor The size of the jitter buffer is Scaling Factor multiplied by packet length or by estimated network jitter (depending on the value of the previous field).

Local Adaptation The jitter buffer modifies its size during silence gaps. This way the change in delay is not noticed by the listener. This parameter determines when to perform this adaptation. The options are:

Off Regard as silence packets only those packets that the far end has marked as such.

On Regard as silence packets both the packets that the far end detected, and the packets that were locally detected as speech gaps.

On with sample interpolation No silence is needed. The adaptation is performed gradually through interpolation, so the listener does not notice the jitter buffer change in size. Notice that for this mode, modem or fax transmission could be distorted. This feature should only be used in the case of voice transmission.

Initial Size The initial size of the jitter buffer (in milliseconds).

Maximum Size The maximum size of the jitter buffer (in milliseconds).

Minimum Size The minimum size of the jitter buffer (in milliseconds).

5.5.8.10 Changing the FXS Ports Settings

The 'FXS Ports' section in the 'Advanced' screen contains advanced electronic settings for the FXS (analog) ports, which should only be modified by an experienced administrator or technician.

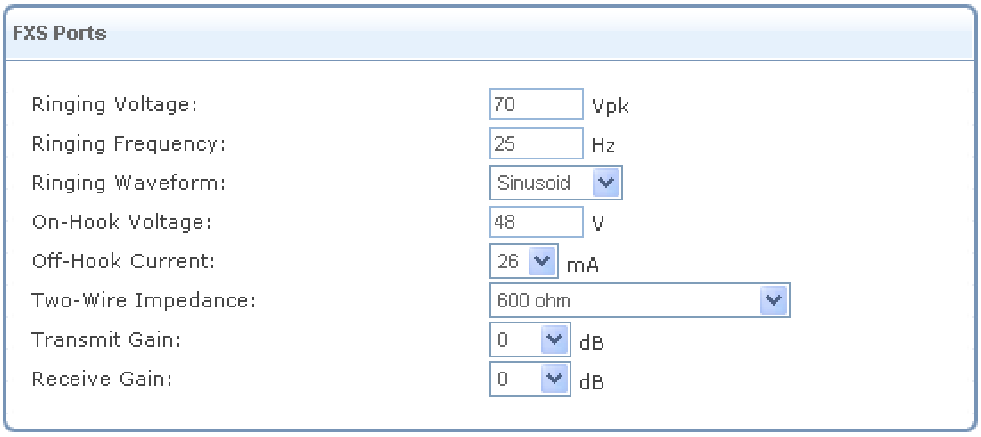


Figure 5.160 Advanced – FXS Ports

Ringing Voltage The ringing voltage in volts.

Ringing Frequency The ringing frequency in hertz.

Ringing Waveform The ringing waveform – sinusoid or trapezoid.

On-Hook Voltage The voltage of an idle handset in volts.

Off-Hook Current Limit The current of an active handset in milli-amperes.

Two-Wire Impedance Select the voice band impedance in ohms, synthesized by the SLIC.

Transmit Gain The transmit gain in decibels.

Receive Gain The receive gain in decibels.

5.5.8.11 Enable Voice

This section allows you to enable or disable OpenRG's Voice module.

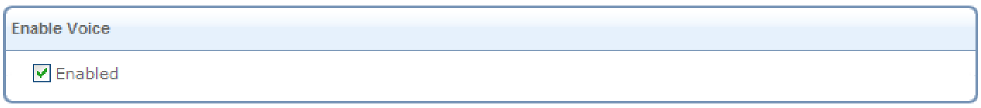


Figure 5.161 Enable Voice

> Note: This feature is only available on gateways with the Asterisk-based Voice module.

To disable the Voice module, deselect the 'Enable Voice' check box, and click 'Apply'. The following message appears in all of the service's configuration screens.

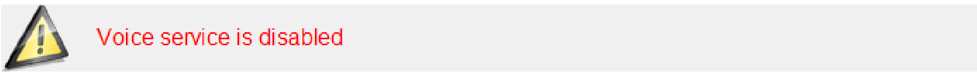


Figure 5.162 Disabled Voice Service

5.6 IP-PBX

OpenRG's Internet Protocol – Private Branch Exchange (IP-PBX) solution provides a private telephone switching system that allows telephone extensions to connect to each other as well as to the outside world.

In most cases, a PBX is an independent piece of equipment residing in an enterprise. Your gateway, however, includes such a PBX, saving you the need to purchase and install an independent PBX. Among the invaluable features of the PBX are its ability to switch calls between users in a network form, as well as share a specific number of external phone lines saving the added cost of designating an external phone line for each user.

OpenRG's PBX manages both Plain Old Telephone Service (POTS) and Voice over IP (VoIP) devices, utilizing VoIP lines to connect them to telephony service providers (proxies). Devices within OpenRG's PBX can freely communicate with each other, thus creating a cost-effective telephony environment.

OpenRG's PBX is available in two different versions—Home PBX and Full PBX. The Home PBX is a lighter version including only the necessities for running a basic PBX in your home, while the Full PBX features vast capabilities aimed at providing you with all aspects of a telephony exchange system. While this section covers the Full PBX, notes are incorporated for features that are not available with the Home PBX version.

Click the 'IP-PBX' menu item under the 'Services' tab. The main IP-PBX screen appears, displaying the available lines and their status.

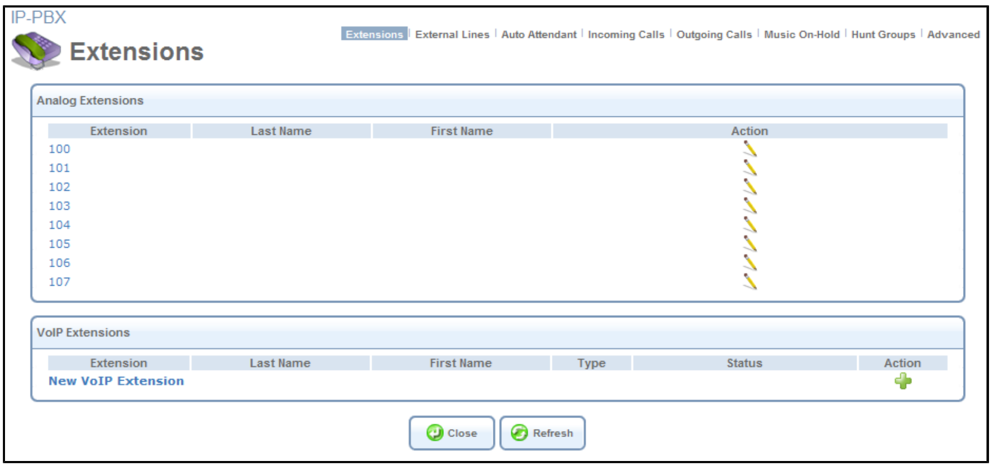


Figure 5.163 IP-PBX Lines

5.6.1 Configuring Your Analog Extensions

To view and edit an analog port's default extension, as well as other settings, click the extension number (or its action icon). The 'Edit Extension' screen appears.

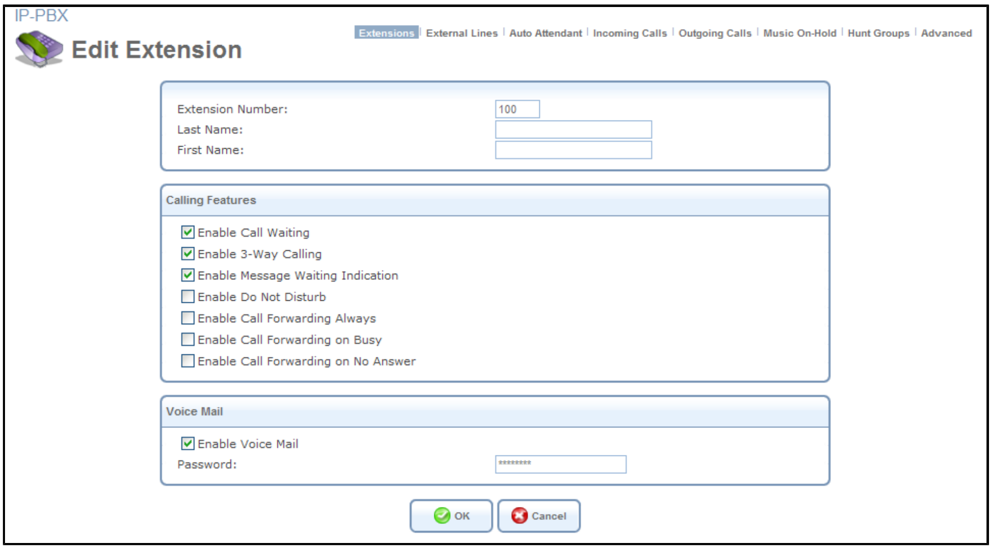


Figure 5.164 Edit Extension

Configure the following parameters:

Extension Number Specify the extension number.

Last Name, First Name Specify a full name for the extension's user.

Enable Call Waiting Select this check box to enable the Call Waiting feature.

Enable 3-Way Calling Select this check box to allow all forms of three-way conversations. When this option is disabled you will not be able to place a call on hold, transfer a call or engage in a call conference.

Enable Message Waiting Indication Select this check box to play a special stutter tone whenever you receive a voice message.

Enable Do Not Disturb Select this check box to prevent calls from reaching your extension. The caller will be forwarded to your voice mail. This feature can also be enabled or disabled by dialing *78 or *79 respectively.

Enable Call Forwarding Always Select this check box to forward incoming calls to another telephone number. The screen refreshes, displaying a field for entering the alternate number.

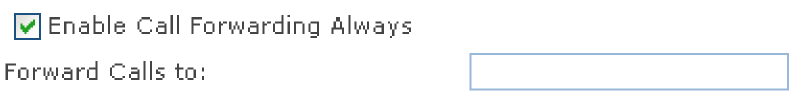


Figure 5.165 Enable Call Forwarding Always

This feature can also be enabled or disabled by dialing *72 (and the alternate number) or *73 respectively.

Enable Call Forwarding on Busy Select this check box to forward incoming calls to another telephone number when the line is busy. The screen refreshes, displaying a field for entering the alternate number.

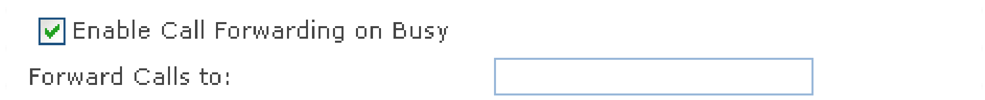


Figure 5.166 Enable Call Forwarding on Busy

This feature can also be enabled or disabled by dialing *90 (and the alternate number) or *91 respectively.

Enable Call Forwarding on No Answer Select this check box to forward incoming calls to another telephone number if the call is not answered within a specific timeframe. The screen refreshes, displaying a field for entering the alternate number, and a field for determining the timeframe to ring before the call is forwarded.

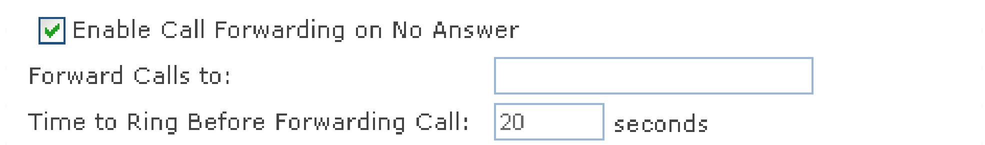


Figure 5.167 Enable Call Forwarding on No Answer

This feature can also be enabled or disabled by dialing *92 (and the alternate number) or *93 respectively.

Enable Voice Mail Enable the voice mail feature. To learn how to use this feature, refer to Section 5.6.9.

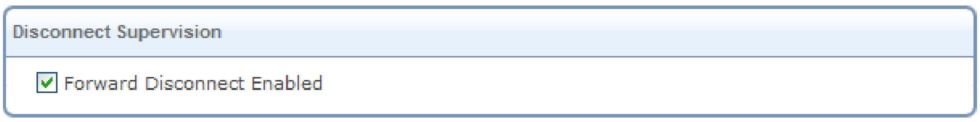


Figure 5.168 Line Parameters – Disconnect Supervision

Note: This feature is only available on Intel IXP425 platforms.

Disconnect Supervision When the 'Forward Disconnect Enabled' check box is selected, the FXS sends a momentary lapse of power to the telephone device whenever the remote party hangs up.

5.6.2 Operating Your Telephone

Following are several guidelines that will help you perform basic telephne operations.

- **Placing a Call**

    1. Pick up the handset on the phone.
    2. Dial the remote party's number (for an external call, begin with **9** and dial '#' to have the call sent out immedately).

- **Answering a Waiting Call**
  When the Call Waiting feature is enabled, you may receive a call while engaged in another call. When such call arrives, you will hear a call waiting tone.

    1. To answer a waiting call, press 'Flash'.
    2. 'Flash' may be used to switch back and forth between calls.

- **Blind Transfer**
  To transfer an existing call (B) to a third party (C) without consultation, perform the following:

    1. Press 'Flash'. Party B will now be placed on hold, and you will hear a dial tone.
    2. Dial party C's number (for an external call, begin with **9** and dial '#' to have the call sent out immedately).
    3. To complete the transfer, place the phone's handset on-hook. B is now initiating a call to C.

- **Call Transfer With Consultation**
  To transfer an existing call (B) to a third party (C), perform the following:

    1. Press 'Flash' on the phone. Party B will now be placed on hold, and you will hear a dial tone.
    2. Dial party C's number (for an external call, begin with **9** and dial '#' to have the call sent out immedately). You can engage in conversation.
    3. To complete the transfer, place the phone's handset on-hook.

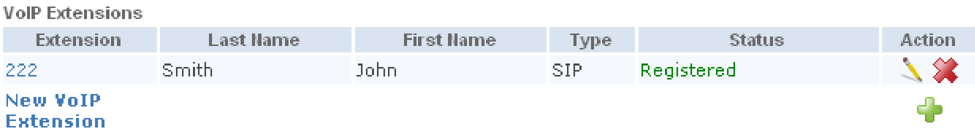
- **3-Way Conference**
  To extend an existing call (B) into a 3-way conference by bringing in an additional party (C), perform the following:

    1. Press 'Flash' on the phone. Party B will now be placed on hold and you will hear a dial tone.
    2. Dial party C's number (for an external call, begin with **9** and dial '#' to have the call sent out immedately). You can engage in conversation.
    3. Press 'Flash' to join both C and B to a single conference.

4. When you place the phone's handset on-hook, party B and party C will remain in conversation.

5.6.3 Connecting VoIP Telephones

Connect a VoIP telephone to an available LAN socket on your gateway. Once connected, you will have to configure the telephone and then add a VoIP extension for it in OpenRG. When done, the status of the extension should change to "Registered".


VoIP Extensions

Extension	Last Name	First Name	Type	Status	Action
222	Smith	John	SIP	Registered	
New VoIP Extension					

Figure 5.169 VoIP Extensions

OpenRG supports both SIP and MGCP VoIP devices. You must be aware of your type of device and configure it accordingly.

5.6.3.1 Configuring Your VoIP Telephone

Configure the telephone with the following settings. Refer to the device's documentation if necessary.

- **SIP Device** – Configure the SIP service provider with OpenRG's IP address (192.168.1.1), and the device's SIP user ID with an extension number of your choice.
- **MGCP Device** – Configure the device's media gateway controller field with OpenRG's IP address (192.168.1.1). In addition, if the device's user ID is configurable, verify that it is set to "aaln/1". Note that if the device has multiple lines, their user ID should be "aaln/1","aaln/2", and so forth.

5.6.3.2 Adding a VoIP Extension

To add a VoIP extension for the IP telephone, click the 'New VoIP Extension' link in the 'Extensions' screen (see Figure 5.163). The 'Edit Extension' screen appears.

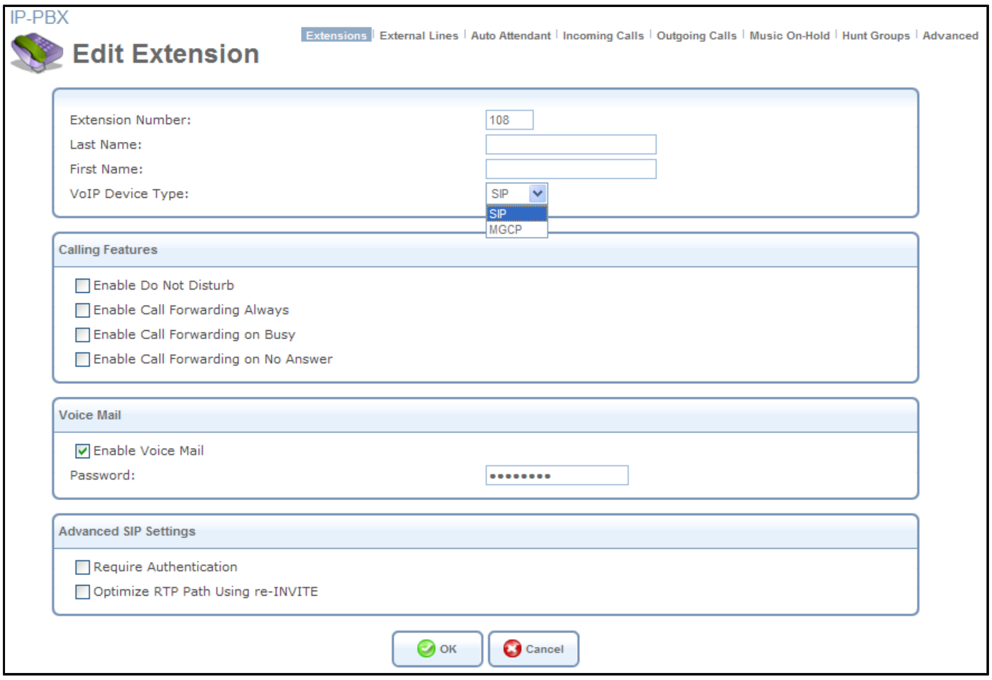


Figure 5.170 Edit Extension – SIP

Configure the following parameters, common to both device types (SIP/MGCP):

Extension Number Specify the extension number, as pre-configured in the device's settings.

Last Name, First Name Specify a full name for the extension's user.

VoIP Device Type Select your device type, SIP or MGCP. The screen refreshes accordingly, and the different parameters are described later in this section.

Enable Do Not Disturb Select this check box to prevent calls from reaching your extension. The caller will be forwarded to your voice mail. This feature can also be enabled or disabled by dialing *78 or *79 respectively.

Enable Call Forwarding Always Select this check box to forward incoming calls to another telephone number. The screen refreshes, displaying a field for entering the alternate number.

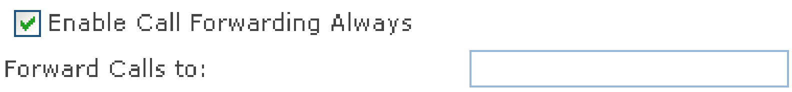


Figure 5.171 Enable Call Forwarding Always

This feature can also be enabled or disabled by dialing *72 (and the alternate number) or *73 respectively.

Enable Call Forwarding on Busy Select this check box to forward incoming calls to another telephone number when the line is busy. The screen refreshes, displaying a field for entering the alternate number.

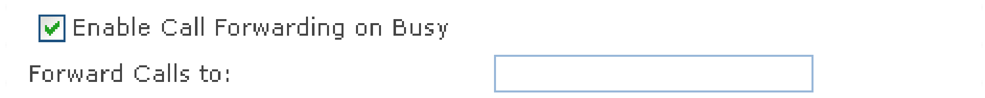


Figure 5.172 Enable Call Forwarding on Busy

This feature can also be enabled or disabled by dialing *90 (and the alternate number) or *91 respectively.

Enable Call Forwarding on No Answer Select this check box to forward incoming calls to another telephone number if the call is not answered within a specific timeframe. The screen refreshes, displaying a field for entering the alternate number, and a field for determining the timeframe to ring before the call is forwarded.

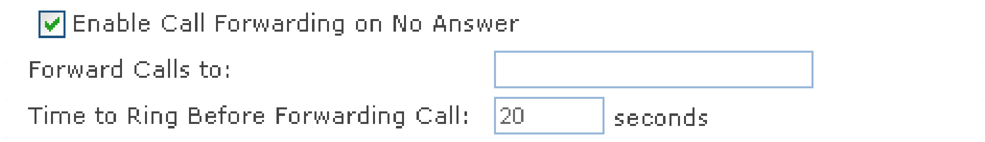


Figure 5.173 Enable Call Forwarding on No Answer

This feature can also be enabled or disabled by dialing *92 (and the alternate number) or *93 respectively.

Enable Voice Mail Enable the voice mail feature. To learn how to use this feature, refer to Section 5.6.9.

5.6.3.2.1 SIP Device Parameters

By default, the 'VoIP Device Type' drop-down menu option is set to SIP. In addition to the general parameters described above, configure the following SIP-specific parameters in the 'Advanced SIP Settings' section.

Require Authentication Select this check box to secure your telephony network. By default, SIP devices register with OpenRG as their proxy (you must configure the device's proxy field with OpenRG's IP address), by identifying themselves with extension numbers, pre-configured on both the devices and on OpenRG. When selecting the 'Require Authentication' option, OpenRG will not accept mere extension number identification, but will require additional authentication data, in the form of a user name and password. This protects your telephony network from, for example, a malicious wireless intruder disguising himself as one of your office extensions, and making free phone calls at your expense. When this option is selected, the screen refreshes, providing username and password fields.

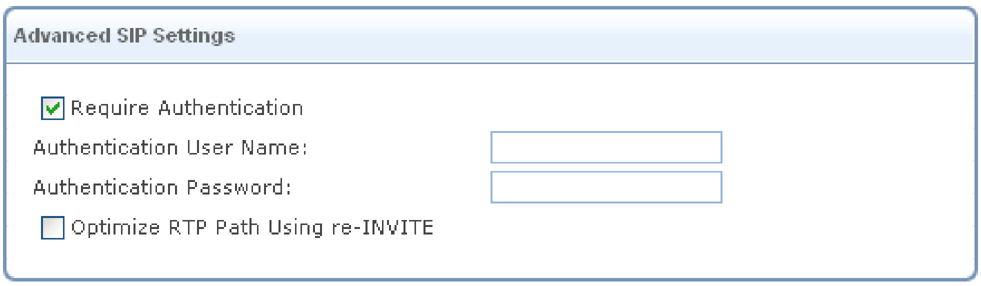


Figure 5.174 SIP Settings

- **Authentication User Name** The user name used for SIP device authentication. Note that this user name must first be configured on the SIP device.

- **Authentication Password** The password used for SIP device authentication. Note that this password must first be configured on the SIP device.

Optimize RTP Path Using re-INVITE Select this option if you would like OpenRG to attempt letting the telephony LAN device and the SIP proxy exchange Real Time Protocol (RTP) traffic (the audio stream) directly, which is more efficient. Note that in order for this feature to work, it must also be enabled for the VoIP line through which the call is routed (refer to Optimize RTP Path Using re-INVITE).

> OpenRG also supports features such as Call Waiting, 3-way Calling, and Message Waiting Indication. However, on a SIP device these features are controlled from the telephone, and therefore non-configurable on OpenRG.

5.6.3.2.2 MGCP Device Parameters

Selecting the MGCP option in the 'VoIP Device Type' drop-down menu refreshes the screen.

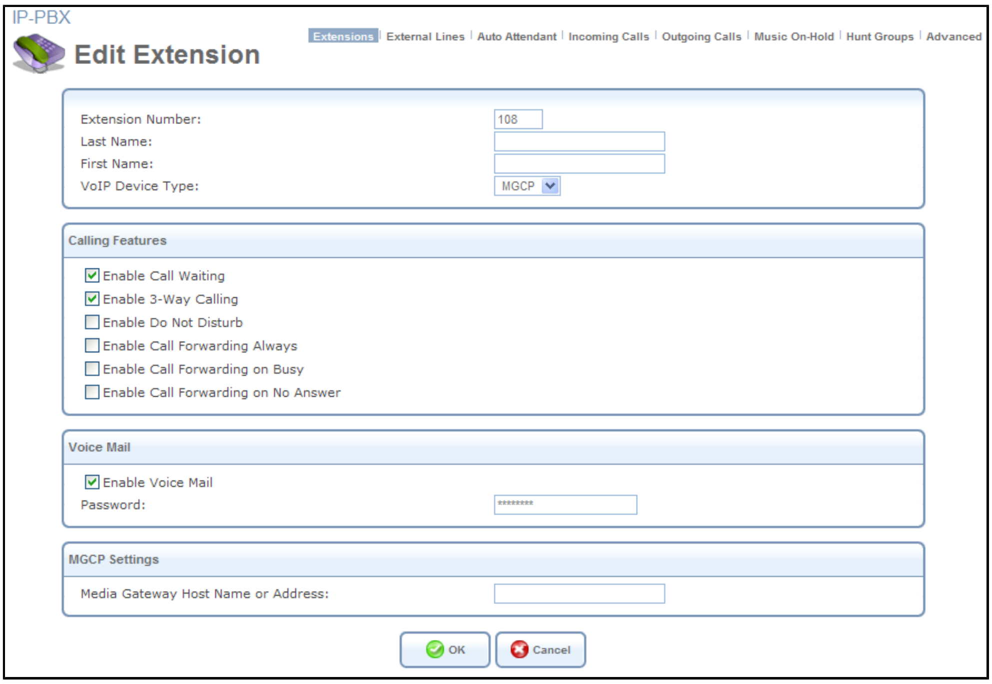


Figure 5.175 Edit Extension – MGCP

In addition to the general parameters described above, configure the following MGCP-specific parameters.

Enable Call Waiting Select this check box to enable the Call Waiting feature.

Enable 3-Way Calling Select this check box to allow all forms of three-way conversations. When this option is disabled you will not be able to place a call on hold, transfer a call or engage in a call conference.

Media Gateway Host Name or Address Specify the telephony device's name or IP address. If the device is connected to OpenRG's LAN, it is recommended to override its dynamic IP address assignment, by pre-configuring it with a static IP address outside OpenRG's range of dynamically-assigned IP addresses. This will avoid its address from changing (in which case you would have to re-enter the new address in this field.)

5.6.4 Opening Telephony Service Accounts

To connect your PBX to the outside world, it is necessary that you obtain a telephony service account, for example a SIP account, as explained in the 'Connecting a Telephone' section of the OpenRG User Manual. This example simulates two separate SIP accounts—one for office use and one for home use. Therefore, open an additional SIP account, either with "FWD" or with another provider of your choice.

In addition to SIP, OpenRG supports the H.323 protocol, which you can obtain as your type of telephony service.

5.6.5 Defining VoIP Lines

After creating telephony accounts and obtaining the necessary details, configure respective VoIP lines, as follows:

1. Click the 'External Lines' link in the PBX main screen (see Figure 5.163). The 'External Lines' screen appears.

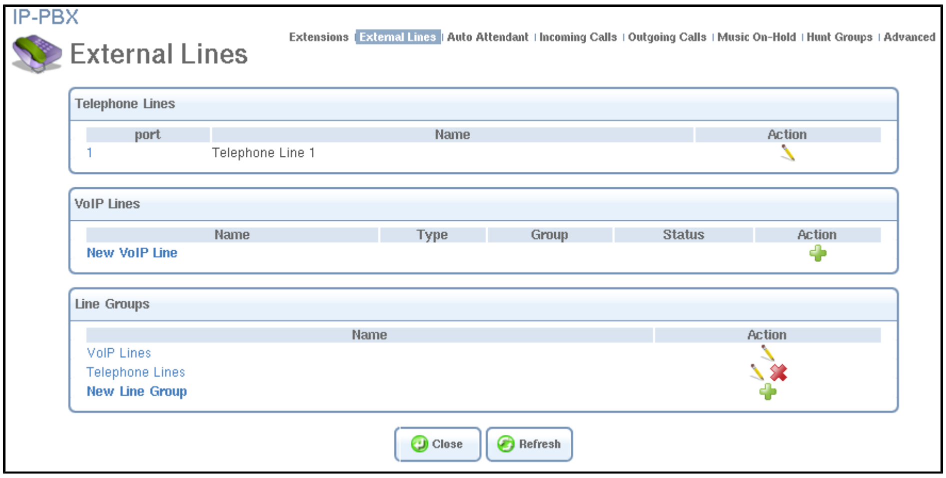


Figure 5.176 External Lines

2. Click the 'New VoIP Line' link. The 'Edit Line' screen appears.

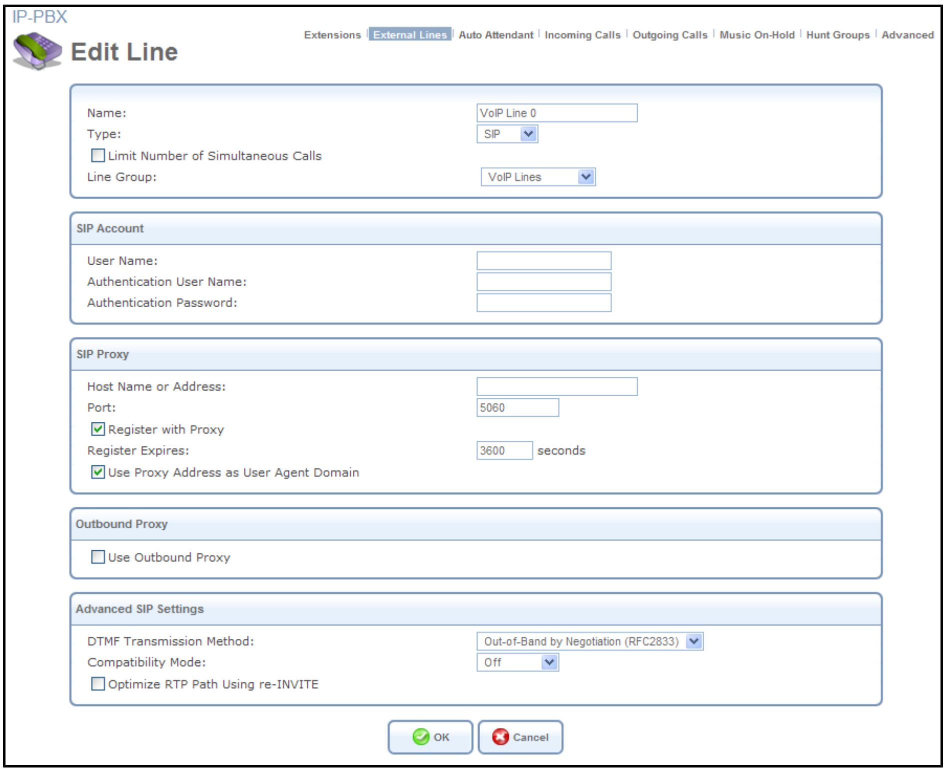


Figure 5.177 Edit Line

3. Configure the following parameters, common to both account types (SIP/H.323). Then, configure the account-specific parameters, as described in the following respective sections.

Name The name of the VoIP line. For example, type "Office" as the name for this VoIP line, as it will simulate your office line.

Type Select the type of VoIP line according to your type of telephony service subscription —SIP or H.323. Their different settings are depicted in the following sections.

Limit Number of Simultaneous Calls You can control the maximum number of simultaneous calls performed from OpenRG through the VoIP line. This is useful, for example, if your telephony account has a call limit. When selecting this option, the screen refreshes, providing a field for entering the maximum number.

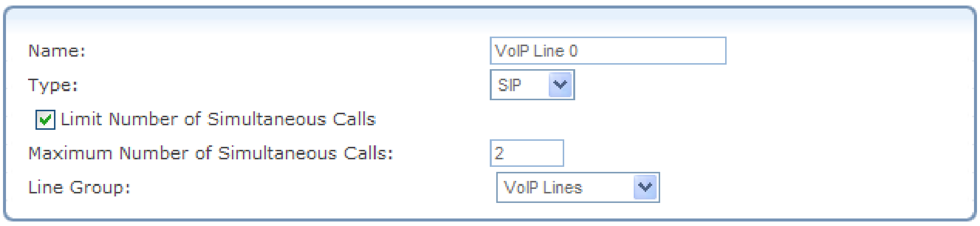


Figure 5.178 Limit Number of Simultaneous Calls

Line Group A group of VoIP lines to which this line belongs. When multiple line groups are defined, use the drop-down menu to select a group to which this VoIP line will belong. To define line groups, refer to Section 5.6.5.3.

5.6.5.1 SIP Account

By default, the 'Type' drop-down menu option is set to SIP. In addition to the general parameters described above, configure the following SIP-specific parameters.

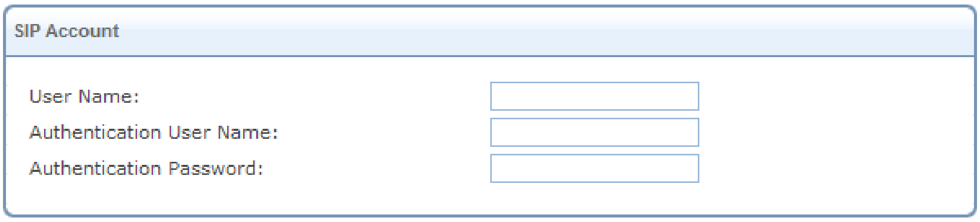


Figure 5.179 Edit Line – SIP Account

User Name Enter your SIP account ID.

Authentication User Name/Password The login name and password used for authentication with the proxy.

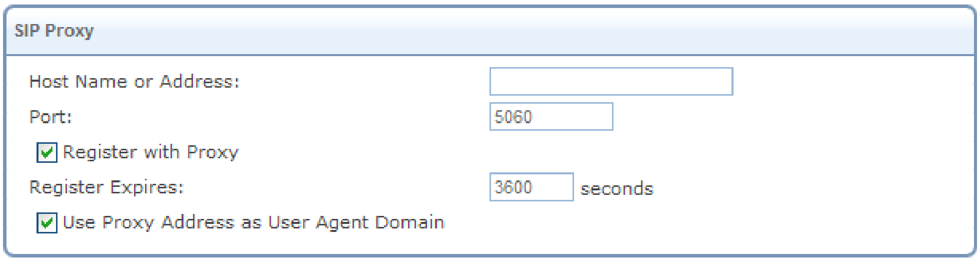


Figure 5.180 Edit Line – SIP Proxy

Host Name or Address Enter the IP address or host name that you received when registering your SIP account. Your free account's host name should be "fwd.pulver.com" (this may vary; you should check your registration e-mail).

Port The port that this proxy is listening on.

Register with Proxy Select this option to register with the proxy, allowing other parties to call OpenRG through it. When this item is checked, the following field becomes visible:

Register Expires The number of seconds between registration renewals.

Use Proxy Address as User Agent Domain Select this option to use the set proxy or its IP address as a domain name specified in outgoing SIP messages. When this option is unchecked, the 'User Agent Domain' field appears. Use this field for setting another proxy address as a user agent domain.

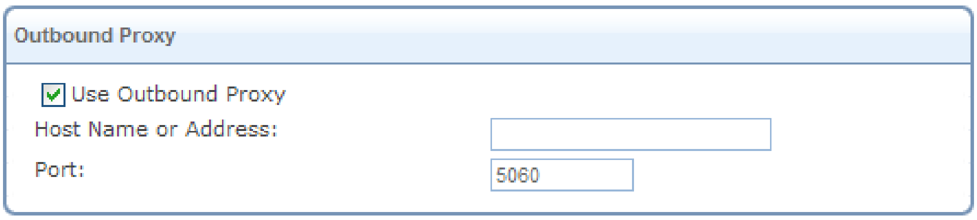


Figure 5.181 Edit Line – Outbound Proxy

Use Outbound Proxy Some network service providers require the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and is the only way to let SIP traffic pass from the internal network to the Internet. The free world-wide dialing service is an example of a service provider that requires the use of an outbound proxy. When this option is checked, the following fields become visible.

Host Name or Address Enter the outbound proxy's IP address or host name that you received when registering your SIP account in the 'Host Name or Address' field. Your free account's outbound proxy's name should be "fwdnat.pulver.com" (this may vary; you should check your registration e-mail).

Port The port on which the outbound proxy is listening. Set this field to 5082 (this may also vary).

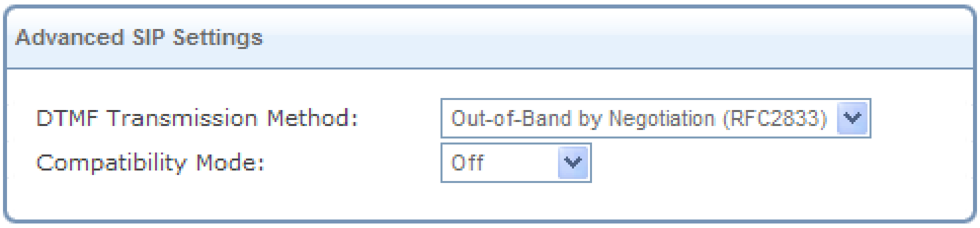


Figure 5.182 Edit Line – Advanced SIP Settings

DTMF Transmission Method Select a transmission method from the drop-down menu:

- **Inband** The DTMF keypad tones are sent within the voice stream.
- **Out-of-Band Always (RFC2833)** The DTMF keypad tones are represented by the keypad number and are sent as separate packets. This is a more reliable transmission method.
- **Q.931 Keypad** The DTMF keypad tones are sent using Q.931 messages.
- **H.245 Alphanumeric** The DTMF keypad tones are sent using an H.245 alphanumeric Information Element (IE).
- **H.245 Signal** The DTMF keypad tones are sent using an H.245 signal IE.
- **Out-of-Band by Negotiation (RFC2833)** This method allows negotiation with the remote party. DTMF tones will be sent either in-band or out-of-band, depending on the remote party's preference.
- **SIP INFO** A special SIP message that includes the DTMF event description.

Compatibility Mode If you are using Broadsoft as your SIP provider, select its mode from this drop-down menu. Otherwise, leave as "Off".

Optimize RTP Path Using re-INVITE Select this option if you would like OpenRG to let the SIP proxy and a telephony LAN device exchange Real Time Protocol (RTP) traffic (the audio stream) directly, which is more efficient.

Verify that the status of the new VoIP line changes to "Registered". Your SIP-based "Office" line is now ready to be used. In the same manner as described above, define another VoIP line named "Home", which will simulate your home line. You may define VoIP lines for as many SIP proxy accounts as you have, designating each account for a different purpose.

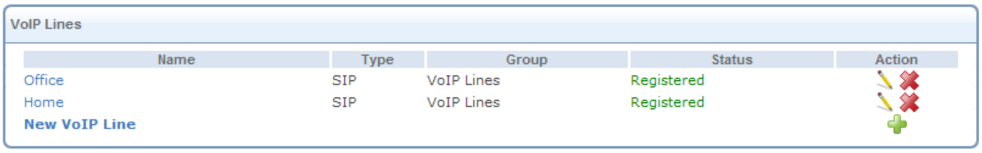


Figure 5.183 VoIP Lines

Note: The 'Telephone Lines' section is currently available on the Broadcom BCM96358 platform only. This section displays an analog (PSTN) line connected via the gateway's Foreign Exchange Office (FXO) port. You can both make and receive phone calls through this line. This is especially useful in case of Internet connectivity problem, when VoIP lines are unavailable.

5.6.5.2 H.323 Account

If you have obtained an H.323 telephony account, select the "H.323" option in the 'Type' drop-down menu of the 'Edit Line' screen (see Figure 5.177). The screen refreshes.

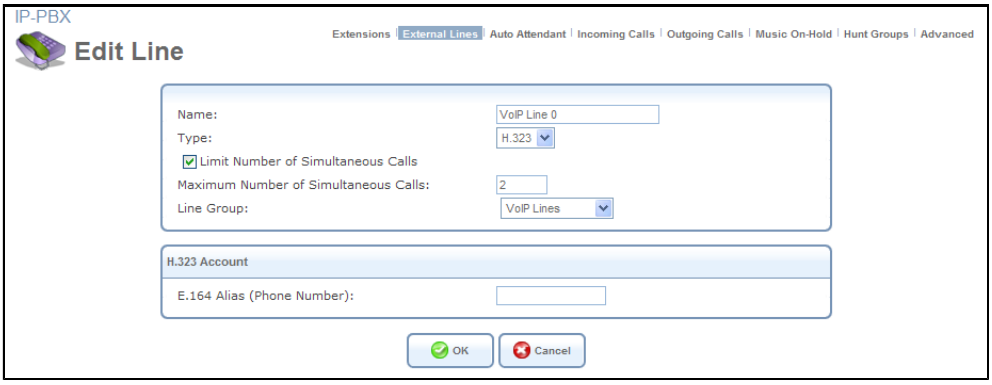


Figure 5.184 Edit Line – H.323

In addition to the general parameters you have already configured above, configure the following H.323-specific parameter.

E.164 Alias (Phone Number) Enter your H.323 account phone number.

5.6.5.3 Grouping Your VoIP Lines

By default, the PBX is pre-configured with one editable, non-removable VoIP line group, to which all created lines will automatically be added. If you would like to distribute your VoIP lines between several groups, simply define additional ones. Click the 'New Line Group'. The 'Edit Line Group' screen appears.

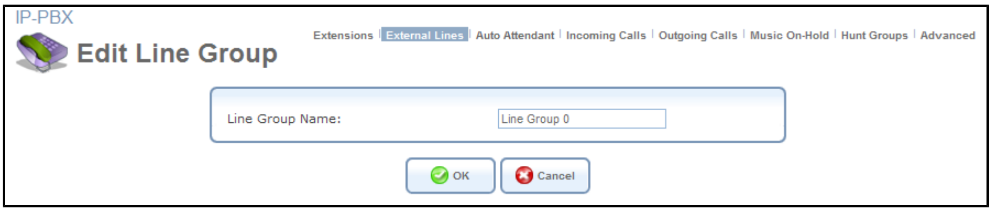


Figure 5.185 Edit Line Group

Enter a name for the new group, and click 'OK' to save your settings. New and existing VoIP lines can now be assigned to each line group, by selecting the group in the 'Line Group' drop-down menu of the 'Edit Line' screen (see Figure 5.177).

5.6.6 Creating Auto Attendants

Note: This feature is only available with the Full PBX version.

OpenRG's PBX includes an auto attendant feature, allowing you to intelligently handle incoming calls, by providing callers the ability to route their calls to relevant parties using the telephone's keypad. You can customize a menu of multiple auto attendants according to your office structure or any other preference. By default, the PBX is pre-configured with one editable, non-removable auto attendant named 'Main Auto Attendant'.

This section depicts an example where the default 'Main' auto attendant is used for an office. Optional auto attendants describe the office location, and inform of the office working hours (an off-hours message). You will first create the optional auto attendants, and then edit the 'Main' attendant with reference to an optional attendant.

1. Create an "Office Directions" auto attendant:

   a. Click the 'Auto Attendant' link in the PBX main screen (see Figure 5.163). The following screen appears.

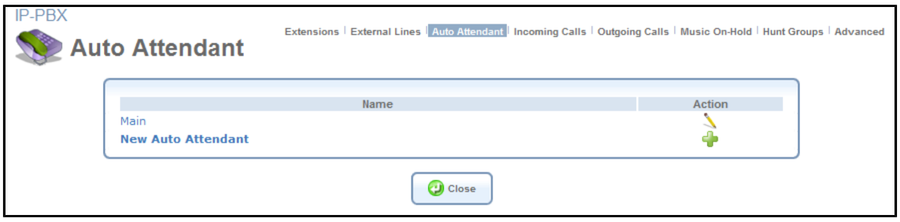


Figure 5.186 Auto Attendant

   b. Click the 'New Auto Attendant' link. The 'Edit Auto Attendant' screen appears.

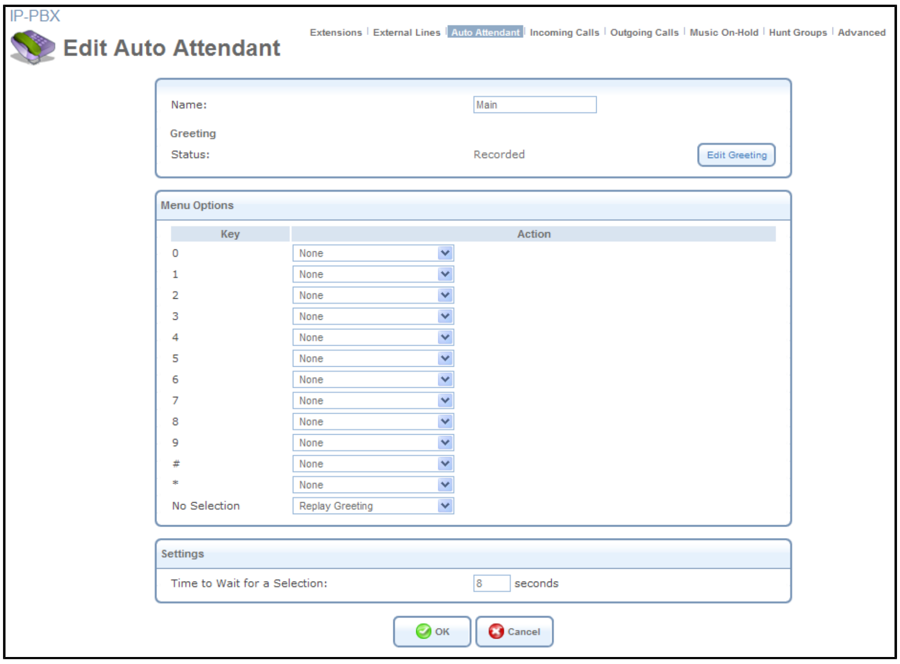


Figure 5.187 Edit Auto Attendant

c. Configure the following parameters:

Name The name of the auto attendant. Type "Office Directions" as the name for this auto attendant.

Greeting The greeting callers will hear when dialing to OpenRG. In order to use OpenRG's default greeting or record your own, you must first connect an external storage device to your gateway. To record your preferred message, click the 'Edit Greeting' button. The 'Auto Attendant Greeting' screen appears.

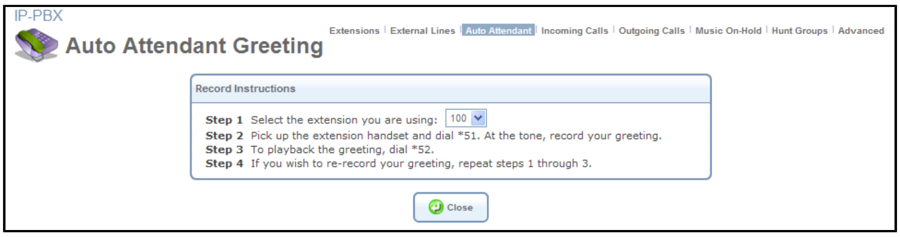


Figure 5.188 Auto Attendant Greeting

Follow the instructions in this screen to record the message directing to your office location. Note that in **Step 1** you must select the extension through which you are recording the message. **Important:** When done, press the 'Close' button.

Menu Options Use this section to configure an action for each keypad button press. This includes the pound and star keys, as well as an action for when no button is pressed. Note that at any time, the caller can dial and be routed to any extension number. The actions that can be defined for every keypad button are:

- **None** No action will be performed.

- **Transfer to Extension** Transfer the call to a specific extension. When defining this action, the screen refreshes, displaying a drop-down menu with all currently available extensions.

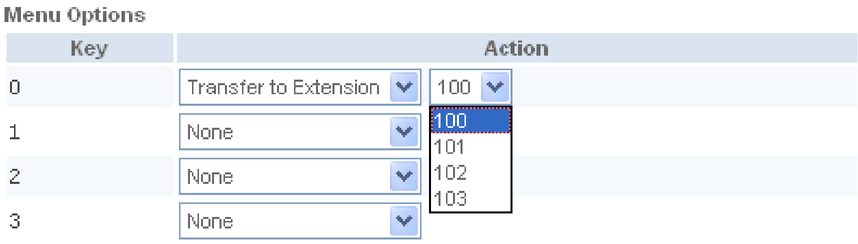


Figure 5.189 Menu Options – Transfer to Extension

- **Play Another Auto Attendant** Transfer to a different auto attendant. This action will only be available when more than one attendant exists. When defining this action, the screen refreshes, displaying a drop-down menu with all other available auto attendants. For example:

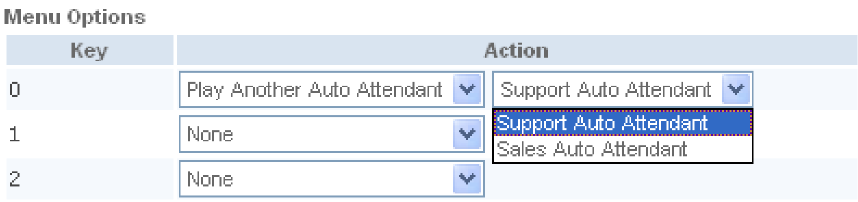


Figure 5.190 Menu Options – Play Auto Attendant

- **Replay Greeting** The greeting message will be replayed.

In the 'No Selection' drop-down menu, select "Play Another Auto Attendant". If the caller does select an action, at the end of the attendant's playback the only other auto attendant available at this time ('Main') will be played. Click 'OK' to save the settings.

Time to Wait for a Selection Specify the timeframe that the system will wait for the caller to select an action. After this timeframe, the action defined in the 'No Selection' menu option will occur.

2. Create a "Working Hours" auto attendant:
   Follow the above procedure to create yet another auto attendant, informing the caller of your office working hours. This auto attendant will be played in the timeframe which you will later on define as non-business hours.
   Important: Skip **Step 6 –** the auto attendant will be replayed until the call is terminated.

3. Edit the 'Main' auto attendant as your main office attendant:

   a. Click the 'Main' auto attendant link. The 'Edit Auto Attendant' screen appears (see Figure 5.187).

   b. Type "Office" as the name for this auto attendant.

c. Select 'Play Another Auto Attendant' for the **5** key (for example). The screen refreshes, displaying an additional combo box.

Figure 5.191 Menu Options – Play Auto Attendant

d. Select the 'Office Directions' auto attendant.

e. Press the 'Edit Greeting' button to record your main office message. This message should include the following directives:

- Inform the caller that he/she may dial an extension number at any time to be transferred to that extension.

- Inform the caller that he/she may press the **5** key to listen to directions on how to get to the office.

f. Click 'OK' to save the settings.

Your auto attendants are now ready to be used.

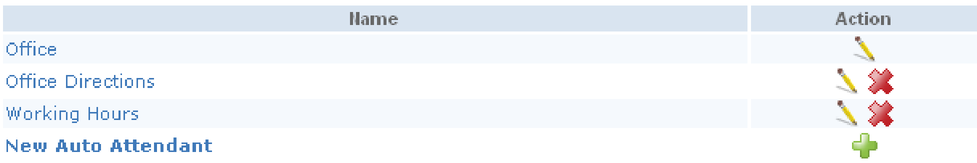


Figure 5.192 Newly Created Auto Attendants

5.6.7 Handling Incoming Calls

OpenRG can receive calls from the telephony proxies associated with its VoIP lines. Such calls will automatically be routed to the PBX through their respective lines. The PBX features an incoming call handling mechanism, enabling you to control your incoming calls per VoIP line, in both day and night modes. This is useful for handling business hours and off-hours calls differently. Since this feature is configured per VoIP line, you must first define one (refer to Section 5.6.5) in order to set its incoming call policy.

After you have created auto attendants, click the 'Incoming Calls' link in the PBX main screen (see Figure 5.163).

Figure 5.193 Incoming Calls

As you can learn from this screen, by default VoIP accounts are configured to play the 'Main Auto Attendant', both day and night, Monday through Friday. Configuring this feature consists of two stages—defining incoming call handling for day and night modes, and scheduling the day mode (which automatically sets the night mode to the rest of the week cycle).

1. Define incoming call handling for day and night modes:

   a. In the 'Incoming Call Handling' section, click the 'Office' VoIP line (or its action icon). The 'Edit Incoming Call Handling' screen appears.

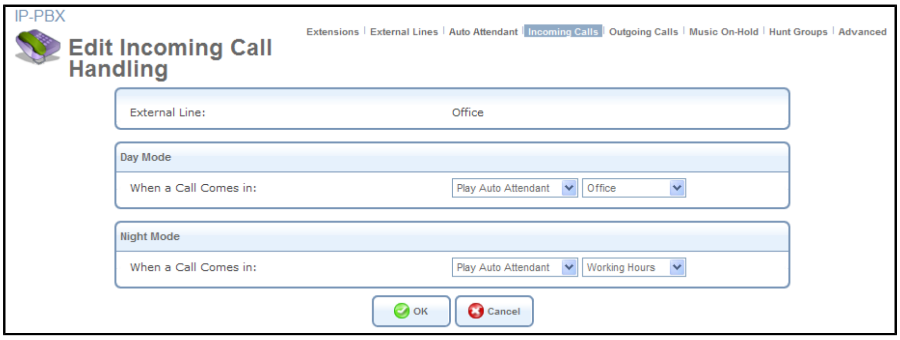


Figure 5.194 Edit Incoming Call Handling

   b. Configure the actions that will occur when a call arrives. The following instructions apply to both day and night modes, which are set in the same manner.

   Play Auto Attendant When this option is selected in the first drop-down menu, the second one displays a list of your available auto attendants.

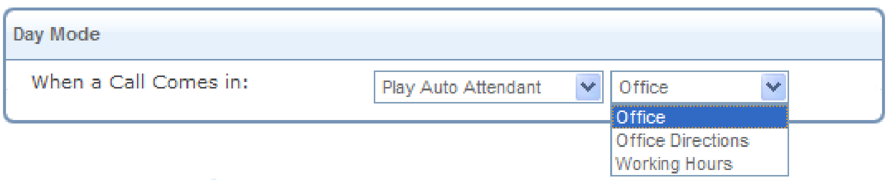


Figure 5.195 Play Auto Attendant

   Select to play the "Office" auto attendant in day mode, and the "Working Hours" auto attendant in night mode. Click 'OK' to save the settings.

Transfer to Extension When this option is selected, the screen refreshes. The second drop-down menu displays a list of your available extensions, to which you can choose to route the call. Additionally, a check box appears.

Play Auto-Attendant If Busy or Unanswered Select this option if you would like to play an auto attendant in case the extension is busy or if the call is unanswered. The screen refreshes again, enabling you to select the auto attendant to be played.

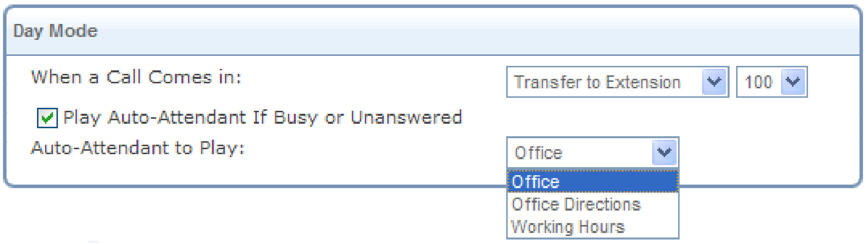


Figure 5.196 Transfer to Extension

c. Back in the 'Incoming Calls' screen, click the 'Home' VoIP line (or its action icon), and configure to transfer incoming calls to extension **100** in both day and night modes. Click 'OK' to save the settings.

2. Scheduling the day mode:
   The 'Day Mode Schedule' section of the 'Incoming Calls' screen (see Figure 5.193) enables you to divide a week cycle into two time segments, during which incoming calls can be handled differently. Only one segment must be configured (the "day" mode), as the rest of the time in the week cycle will be referred to as the second segment (the "night" mode). Determine the day mode time segment:

   Days of Week Select from which day through which day will be included in this mode.

   Hours Range Enter from what hour to what hour of every day will be included in this mode.

Your incoming call handling plan should be as follows:

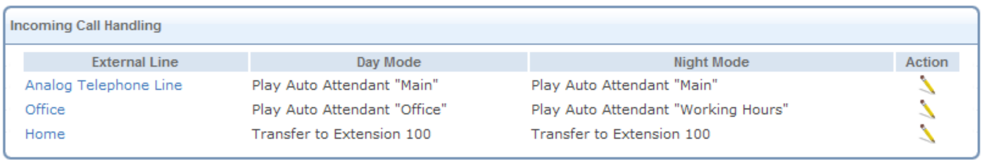


Figure 5.197 Incoming Call Handling

- When a call arrives through the office VoIP line in business hours, the main "Office" attendant will be played, prompting the user to dial any extension number or to press **5** for instructions on how to get to the office. To experience this, you can use the home extension to dial "9" and then your office VoIP line number.

- When a call arrives through the office VoIP line in off-hours, the "Working Hours" attendant will be played, informing the caller of your business hours.

- When a call arrives through the home VoIP line, it will automatically be transferred to extension **100**. To experience this, you can use the office extension to dial "9" and then your home VoIP line number.

5.6.8 Handling Outgoing Calls

OpenRG's PBX provides a sophisticated mechanism for handling outgoing calls, by utilizing a *Dial Plan*. A dial plan is a set of rules you can determine in order to route outgoing calls through specific VoIP lines. Each dial plan rule is referred to as a "dial plan entry", which you can add, edit or remove.

The dial plan mechanism enables you to manipulate the number dialed by the caller, by adding or omitting digits. This can be used for various purposes, such as reaching an external line, replacing telephony proxies' dialing codes, and even defining speed dial shortcuts. To define a new dial plan entry, click the 'New Dial Plan Entry' link. The 'Edit Dial Plan Entry' screen appears (see Figure 5.199).

Click the 'Outgoing Calls' link in the PBX main screen (see Figure 5.163). The following screen appears.

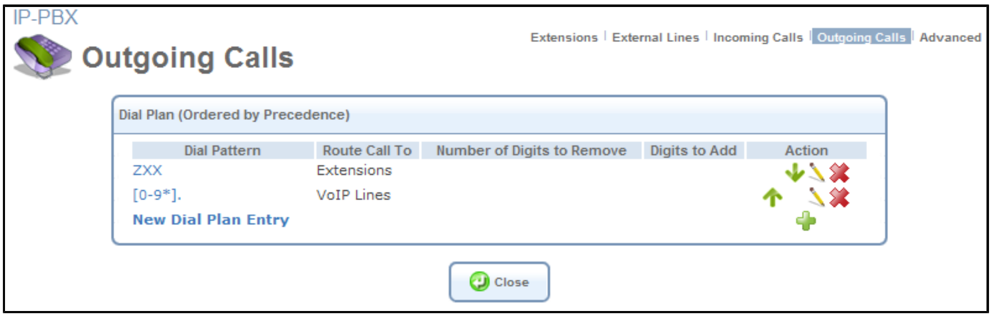


Figure 5.198 Outgoing Calls

The default entries are designed to handle the most common call patterns. Click the 'ZXX' entry (or its  action icon). The 'Edit Dial Plan Entry' screen appears.

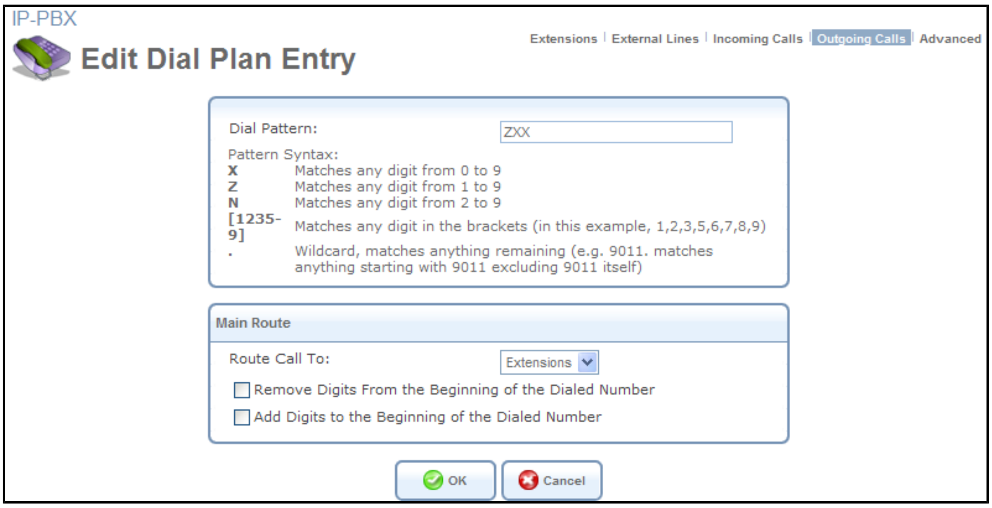


Figure 5.199 Edit Dial Plan Entry

This screen is divided into two main sections–'Dial Pattern', used for setting the variable for dialed numbers, and 'Main Route', used for determining the routing behavior. "ZXX" is a variable for a dial pattern of three digits, where the first is between 1 and 9 and the second and third are between 0 and 9. This pattern covers all extension numbers. When a caller from any extension dials a number that matches this dial pattern, the PBX will route the call to the relevant extension. Similarly, the "[0-9*]." dial pattern is a variable for any number of digits that when dialed, the call will be routed to an external line through the default 'VoIP Lines' group.

As you have obtained an FWD SIP account in previous examples, you may want to use the dial plan to overcome an FWD limitation. As a rule, FWD requires dialing " ***** " (asterisk) as a prefix to 1-800 numbers. Failure to do so will result in an FWD voice message explaining this requirement. To override this limitation, add the following entry to the dial plan.

1. In the 'Outgoing Calls' screen (see Figure 5.198) click the 'New Dial Plan Entry' link. The 'Edit Dial Plan Entry' screen appears.

2. Enter "91800XXXXXXX" as the dial pattern. This pattern represents every possible 1-800 number, dialed after "9" (for an external call), and complies with the specified pattern syntax.

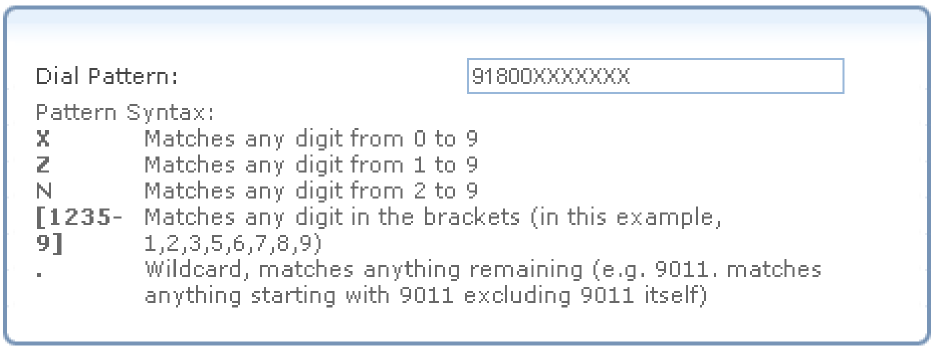


Figure 5.200 Dial Pattern

3. In the 'Main Route' section, configure the following:

Line Group to Use Select the line group through which you would like to route the call. In this example, select "VoIP Lines".

Remove Digits From the Beginning of the Dialed Number Select this option to ignore one or more of the digits specified in the dial pattern before dialing the telephone number. When this option is selected, the screen refreshes, adding the following field:

Number of Digits to Remove Verify that the value of this field is 1.

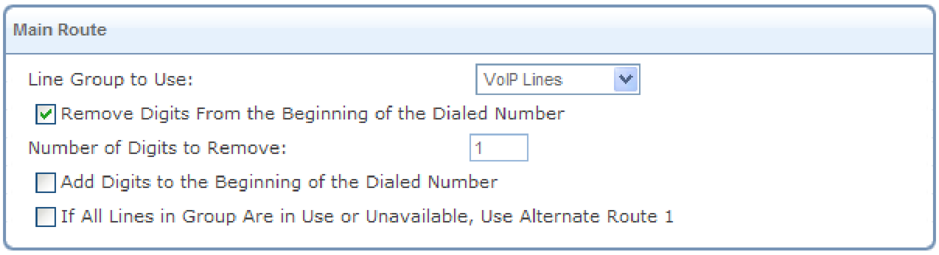


Figure 5.201 Number of Digits to Remove

Add Digits to the Beginning of the Dialed Number Select this option to add digits before dialing the telephone number. When this option is selected, the screen refreshes, adding the following field:

Digits to Add Enter an " ***** " (asterisk) as the digit to be added.

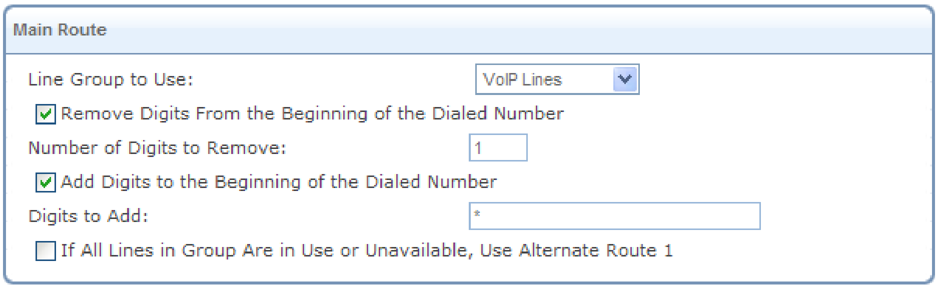


Figure 5.202 Digits to Add

If All Lines in Group Are in Use or Unavailable, Use Alternate Route 1 Select this option to provide an alternate route for the dialed call, in case all lines in the specified line group are in use (this step is not mandatory for the current example). When this option is selected, the screen refreshes, adding the following section:

Alternate Route 1 This section is identical to the 'Main Route' section above, enabling you to select a different set of parameters, thus expanding a call's routing options. You can further select the alternate route option, to create Alternate Route 2, and so on.

Note: On the Broadcom BCM96358 platform, this screen section is enabled by default, and the 'Telephone Lines' group (analog lines) is selected. This is useful if the Internet connection is down, in which case all the VoIP lines are

unavailable. In such a case, a dialed external call will be routed by default to the analog (PSTN) line via an FXO port.

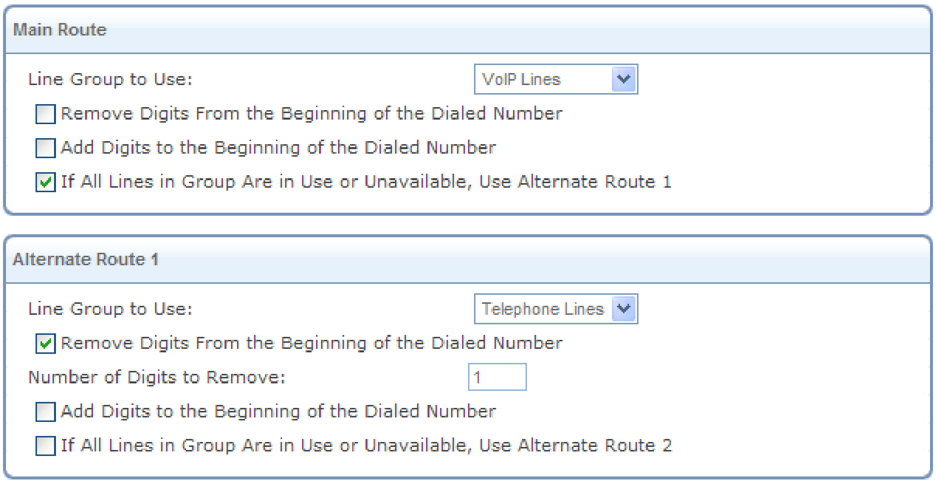


Figure 5.203 Alternate Route 1

4. Click 'OK' to save the settings.

The dial plan entry is added to the 'Outgoing Calls' screen, and is applied on all VoIP lines in the line group selected (in this case, the default 'VoIP Lines' group).

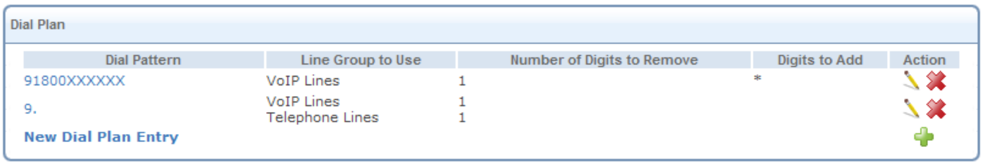


Figure 5.204 Dial Plan

Calls dialed from OpenRG to 1-800 numbers will now be automatically converted into the format required by FWD, concealing its limitation and simplifying telephony operability.

5.6.9 Using the Voice Mail

Note: This feature is only available with the Full PBX version.

The voice mail feature is an interactive attendant application, enabling you to listen to your messages and configure various voice mail options.

5.6.9.1 Accessing the Voice Mail

Every extension features its own voice mailbox. The PBX will indicate that you have messages by commencing the dial tone with a stutter when you pick up the handset. To access an extension's voice mail application, perform the following:

1. Pick up the handset, and dial ***1234**. An attendant will ask for a password.

2. Dial your password. The default password is **0000#**.

As soon as you enter the voice mail application, the attendant will inform you whether you have any messages, and prompt you to press different keys for various mail options. Navigate through these options to perform all voice mail operations.

5.6.9.2 Voice Mail Operations

Following are the available voice mail operations and their corresponding keys. Sub-options are marked with bullets.

1 – New/old messages

- **4** – Play previous message
- **5** – Repeat current message
- **6** – Play next message
- **7** – Delete current message
- **8** – Forward message to another mailbox
- **9** – Save message in a folder
- ***** – Help; during message playback: rewind
- **#** – Exit; during message playback: fast-forward

2 – Change folders

3 – Advanced options

- **1** – Send reply
- **2** – Call back
- **3** – Envelope
- **4** – Outgoing call
- **5** – Leave message
- ***** – Return to main menu

0 – Mailbox options

- **1** – Record your "unavailable" message
- **2** – Record your "busy" message

- **3** – Record your name
- **4** – Change your password
- ***** – Return to the main menu

***** – Help

– Exit

5.6.9.2.1 An Example – Reaching an External Line

In this example you will add an entry that provides the option to press "9" for an external line.

1. Click the 'New Dial Plan Entry' link. The 'Edit Dial Plan Entry' screen appears.

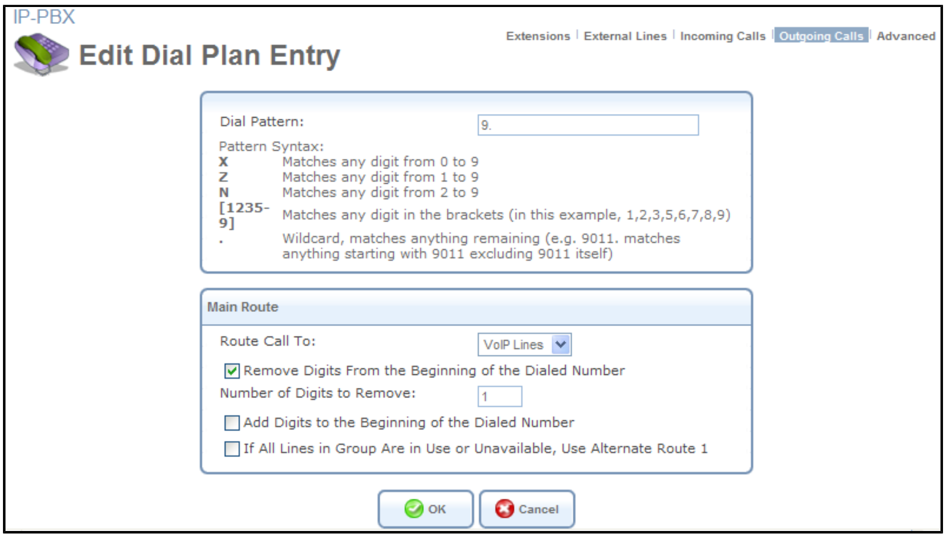


Figure 5.205 Edit Dial Plan Entry

2. In the 'Dial Pattern' field, enter "9."
3. In the 'Route Call To' field select "VoIP Lines".
4. Select the 'Remove Digits From the Beginning of the Dialed Number' check box. The screen refreshes, and the 'Number of Digits to Remove' line is added with a value of 1.
5. Click 'OK' to save the settings.

According to this dial plan entry, when a caller dials "9", the call will be routed to an external line through the default 'VoIP Lines' group, and the dialed "9" digit will be omitted. The caller will then be able to place an external call by simply dialing the desired telephone number.

5.6.10 Adding On-Hold Music Files

Note: This feature is only available with the Full PBX version.

While callers are placed on hold, they will hear background music playing. In order to use OpenRG's default music or upload your own music files, you must first connect an external storage device to your board. To upload an on-hold music file, perform the following:

1. Click the 'Music On-Hold' link in the PBX main screen (see Figure 5.163). The following screen appears.

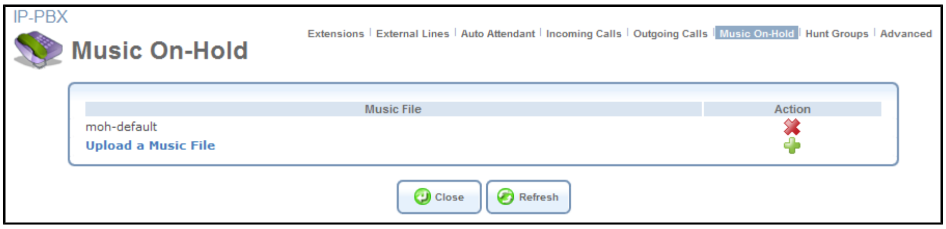


Figure 5.206 Music On-Hold

2. Click the 'Upload a Music File' link. The following screen appears.

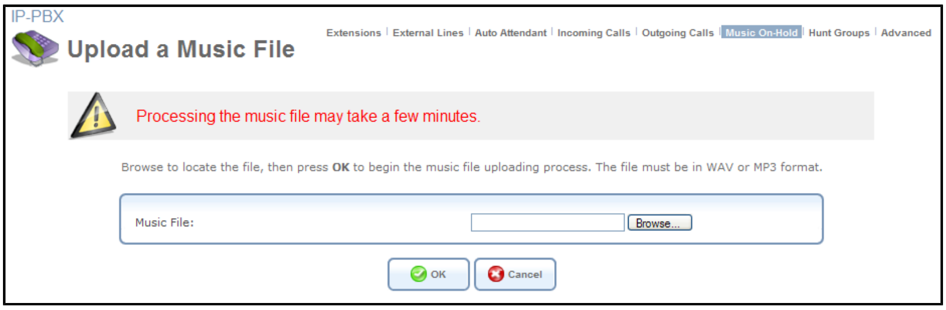


Figure 5.207 Browse For a Music File

3. Click the 'Browse' button to open a browsing window on your computer and select the WAV or MP3 format file to upload.

4. Click 'OK' to begin the upload. Note that this may take several minutes, depending on the size of your file(s).

5.6.11 Automating Call Distribution with Hunt Groups

Note: This feature is only available with the Full PBX version.

Your PBX features *Hunt Groups* for automating distribution of incoming calls to two or more extensions. This allows you to set up groups of operators in order to handle different types of inquiries. For example, you may distribute calls to a **sales hunt group** and a **support hunt group**. Moreover, you can control the distribution of calls within a hunt group in a particular order if an extension is busy or unavailable.

Since hunt groups are groups of extensions, once defined they become optional call recipients. The option "Transfer to Hunt Group" will be added as a menu option in the 'Edit Auto

Attendant' screen (see Figure 5.208) and in the 'Edit Incoming Call Handling' screen (see Figure 5.209).

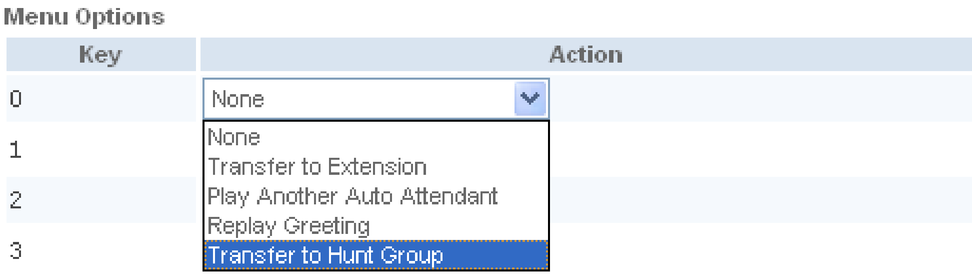


Figure 5.208 Edit Auto Attendant

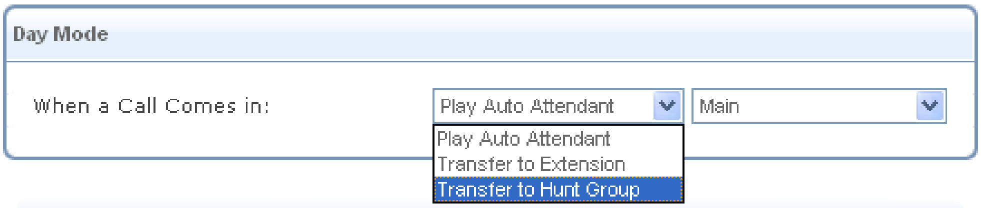


Figure 5.209 Edit Incoming Call Handling

To define a hunt group, click the 'Hunt Groups' link in the PBX main screen (see Figure 5.163). The following screen appears.

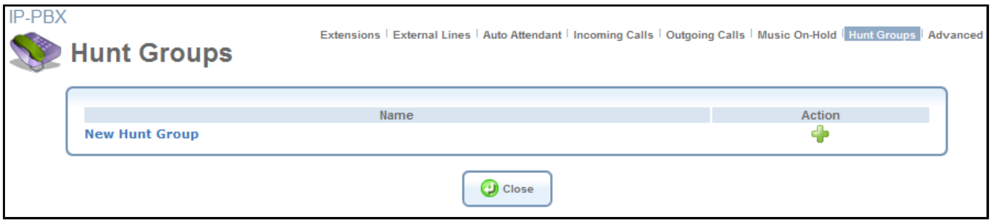


Figure 5.210 Hunt Groups

Click the 'New Hunt Group' link. The following screen appears.

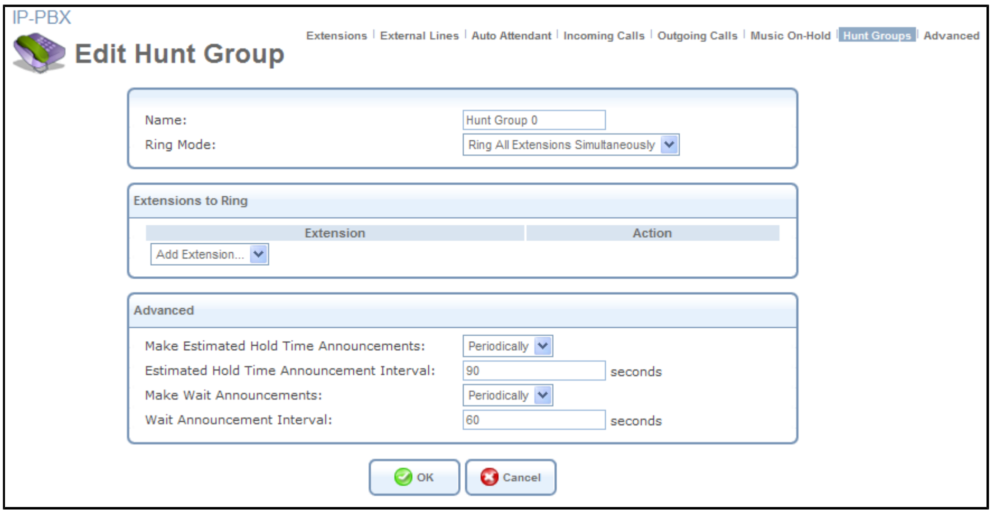


Figure 5.211 Edit Hunt Group

Name The name of the hunt group.

Ring Mode Select whether to ring all extensions at once when a call arrives, where the first operator to answer will accept the call, or to ring one extension at a time in an orderly fashion. Selecting the second choice will refresh the screen.

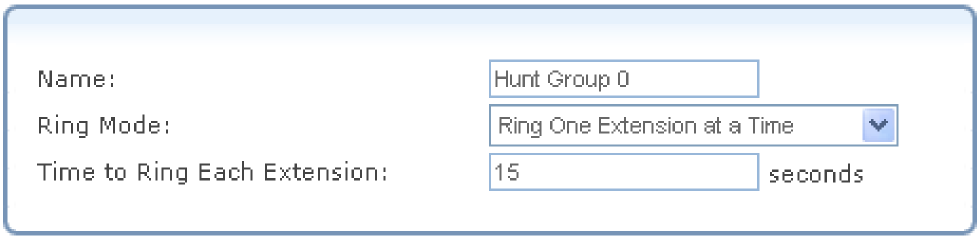


Figure 5.212 Hunt Group Ring Mode

Time to Ring Each Extension Enter the timeframe in which the call will ring on each extension before being routed to the next.

Extensions to Ring Select the extensions that will participate in this hunt group. The drop-down menu will display all of your available extensions. Note that this step is mandatory, otherwise the hunt group is empty. If you had chosen to ring one extension at a time as your ring mode, by default the ring will be routed between the extensions in their order of appearance in this table. When adding multiple extensions, the action icon and action icon appear, allowing you to easily change the order of the extensions. If you had chosen simultaneous rings, the order of extensions is not relevant.

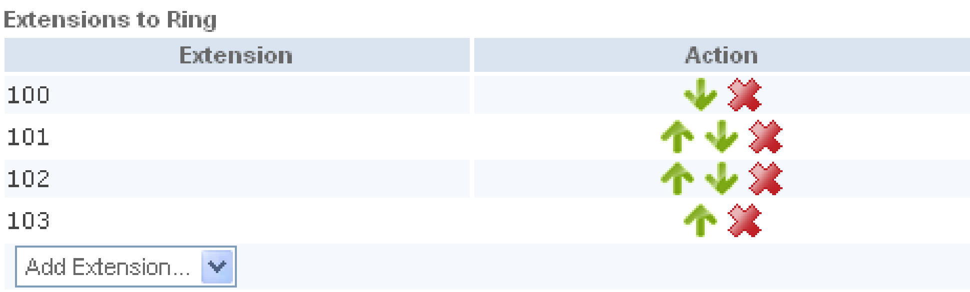


Figure 5.213 Extensions to Ring

Ring Order The ringing cycle order, used to determine the cycle's starting point, or which extension will ring first. This field appears only if you had chosen to ring one extension at a time as your ring mode. In this mode, the extensions will ring one after the other in a cyclic manner, according to their order in the 'Extensions to Ring' table. Select the ring order algorithm to be used:

- Round Robin – The extensions take orderly turns at being the first extension to ring. The order of the turns is the same order defined for the ringing cycle.
- Least Recent – The first extension to ring is the one that has been idle for the longest time.
- Random – The first extension to ring will be chosen randomly.

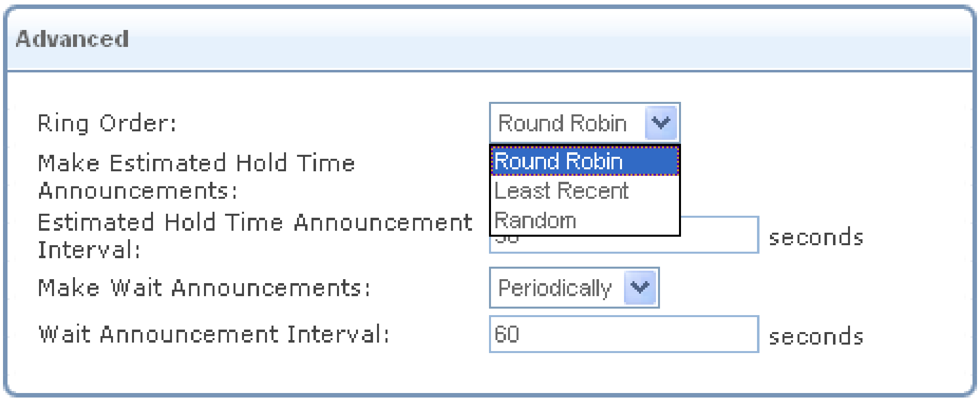


Figure 5.214 Ring Order

Make Estimated Hold Time Announcements Hold time announcements include messages asking the callers to hold, as well as informing the callers of their number in the queue of calls. These messages are played in addition to the on-hold music played in the background. Select whether to play these messages periodically, once, or not at all.

Estimated Hold Time Announcement Interval Enter the number of seconds before the hold time announcements will be repeated. Note that if you had chosen to play the announcements once or not at all, this field will not be visible.

Make Wait Announcements Wait announcements are messages asking the caller to hold. Select whether to play this message periodically or not at all.

Wait Announcement Interval Enter the number of seconds before the wait announcement will be repeated. Note that if you had chosen not to play the announcement at all, this field will not be visible.

Note: When an external caller is transferred to a relevant hunt group without dialing a specific hunt group's extension, the calling features of the reached extension (such as call waiting, call forwarding, etc.) are not activated. This is done in order to automatically transfer the call to the next hunt group's extension, if the previously called extension does not answer. In contrast, when a specific hunt group's extension is requested, its calling features are activated, and the call is not transferred further within the hunt group when the dialed extension does not answer.

5.6.12 Advanced Telephony Options

The 'Advanced' screen enables configuration of advanced settings. Some of these settings are platform-specific, and therefore may not be available with your gateway's software.

5.6.12.1 Configuring Voice Mail Attributes

Note: This feature is only available with the Full PBX version.

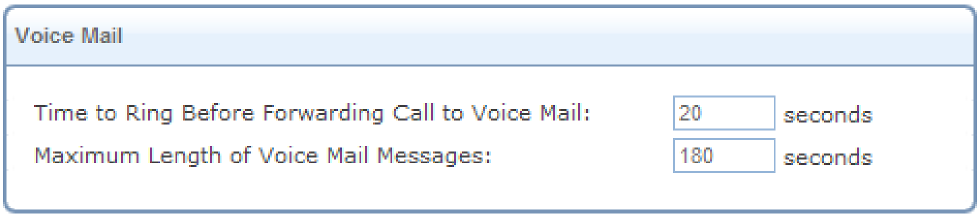


Figure 5.215 Advanced – Voice Mail

Time to Ring Before Forwarding Call to Voice Mail The timeframe in seconds until the call will be forwarded to the voice mail.

Maximum Length of Voice Mail Messages The maximal length in seconds of a message that can be recorded.

5.6.12.2 Switching Extensions with Call Park

Note: This feature is only available with the Full PBX version.

Call parking allows you to put a call on hold at one extension and continue the conversation from any other extension on your PBX.

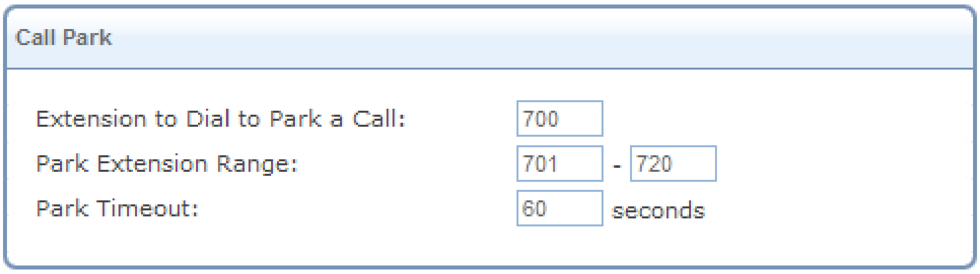


Figure 5.216 Advanced – Call Park

Extension to Dial to Park a Call The extension number that must be dialed in order to park the call. When dialing this number, a voice recording will say a parking extension number that you must dial from any other extension on the PBX in order to resume the parked call.

Park Extension Range The range of parking extension numbers that are available for the system to provide a caller parking a call.

Park Timeout The duration (in seconds) for which the call is parked. During this timeframe, the call can be picked up from any extension on the PBX by dialing the parking extension number provided. After this timeframe, the extension from which the call was parked will ring to resume the call.

5.6.12.3 Setting the SIP Port

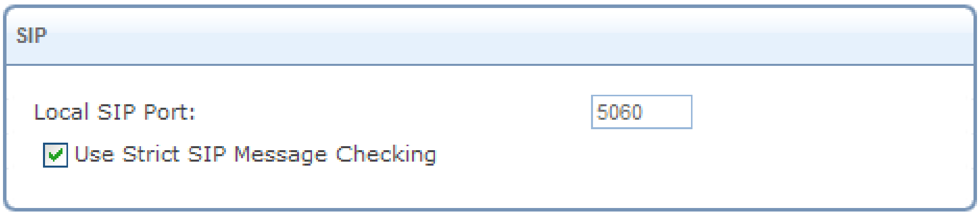


Figure 5.217 Advanced – SIP

Local SIP Port The port on OpenRG that listens to SIP requests from the proxy. By default, port 5060 is used for SIP signaling of phones connected to the gateway. A common problem occurs when using a SIP agent on the LAN (for example, an IP phone). A SIP agent requires port forwarding configuration (refer to Section 5.2.3), which uses the same port—5060. This multiple use of the port causes failure of either or both services. Therefore, when configuring port forwarding for a SIP agent, you must change OpenRG's SIP port value (for example, to 5062). Note that the calling party must be made aware of this value when initiating a direct call (not using a proxy).

5.6.12.4 Configuring H.323 Parameters

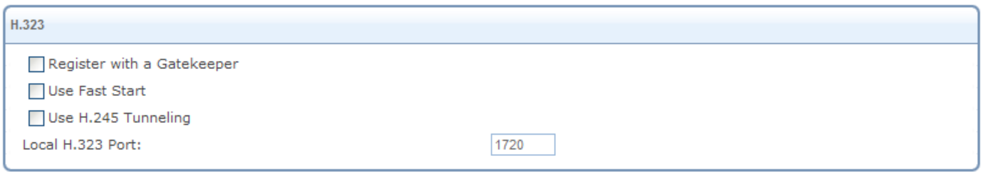


Figure 5.218 Advanced – H.323

Register with a Gatekeeper Register the user with a gatekeeper, allowing other parties to call the user through the gatekeeper. When this item is checked, the following fields become visible:

Gatekeeper Address The IP address or name of the primary gatekeeper.

Gatekeeper Port The port on which the primary gatekeeper is listening for connections.

Specify Gatekeeper ID Select whether a gatekeeper ID should be used for the primary H.323 gatekeeper.

Gatekeeper ID The identifier for the primary H.323 gatekeeper.

Registration Time to Live Specify the valid duration of the H.323 gatekeeper registration in seconds.

Use Alternate Gatekeeper Select this check-box to configure an alternate gatekeeper for redundancy. When this item is checked, the following fields become visible:

Alternate Gatekeeper Address The IP address or name of the alternate gatekeeper.

Alternate Gatekeeper Port The port on which the alternate gatekeeper is listening for connections.

Use Fast Start The fast start connection method can result in quicker connection establishment, depending on the remote party's settings. Note that Microsoft NetMeeting does not support this option, so in order to interoperate with Microsoft NetMeeting, you should disable the feature.

Use H.245 Tunneling Indicates whether H.245 packets should be encapsulated within H.225 packets.

Local H.323 Port Specify the port number to use for H.323 signaling.

DTMF Transmission Method DTMFs are the tones generated by your telephone's keypad.

- **Inband** The DTMF keypad tones are sent within the voice stream.
- **Out-of-Band Always (RFC2833)** The DTMF keypad tones are represented by the keypad number and are sent as separate packets. This is a more reliable transmission method.
- **Q.931 Keypad** The DTMF keypad tones are sent using Q.931 messages.
- **H.245 Alphanumeric** The DTMF keypad tones are sent using an H.245 alphanumeric Information Element (IE).
- **H.245 Signal** The DTMF keypad tones are sent using an H.245 signal IE.

5.6.12.5 Setting the MGCP Port

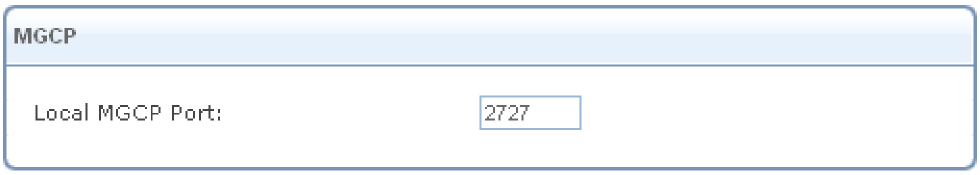


Figure 5.219 Advanced – MGCP

Local MGCP Port The port OpenRG uses for MGCP connections.

5.6.12.6 Selecting Audio Codecs

Audio codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For example, G.723 is a codec that uses compression, so it is good for use where bandwidth is limited but its voice quality is not as good compared to other codecs such as the G.711.

To select the audio codecs, click the 'Advanced' link under the 'Voice' item menu. In the 'Codecs' section, configure the following options.

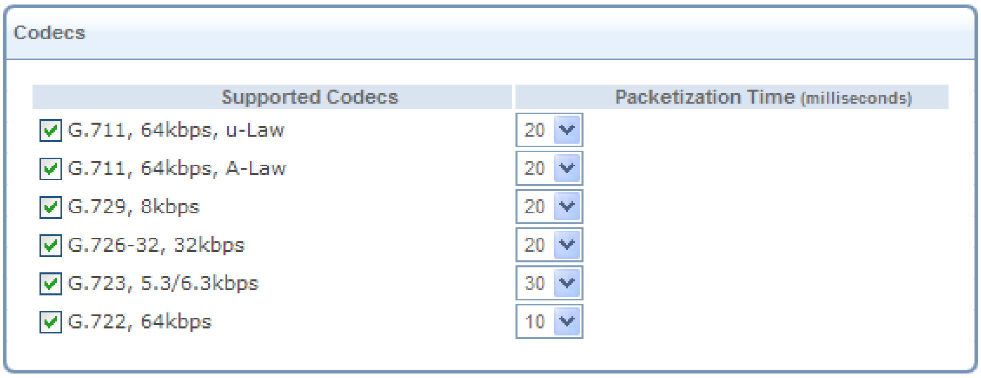


Figure 5.220 Advanced – Codecs

Supported Codecs In order to make a call, at lease one codec must be enabled. Moreover, all codecs may be enabled for best performance. When you start a call to a remote party, your available codecs are compared against the remote party's, to determine which codec will be used. The priority by which the codecs are compared is according to the descending order of their list, as depicted in the figure above. If there is no codec that both parties have made available, the call attempt will fail. Note that if more than one codec is common to both parties, you cannot force which of the common codecs that were found will be used by the remote party's client. If you do wish to force the use of a specific codec, leave only that codec checked.

Packetization Time The Packetization Time is the length of the digital voice segment that each packet holds. The default is 20 millisecond packets. Selecting 10 millisecond packets enhances the voice quality, as less information is lost due to packet loss, but doubles the load on the network traffic.

Note: This feature is only available with the Home PBX version. The Full version of PBX utilizes only the **G.711 u-LAW** codec, which cannot be changed or disabled from the WBM.

5.6.12.7 Changing the Reserved RTP Port Range

The voice stream is transmitted in Real Time Protocol (RTP) packets, which require a range of open ports. If the default ports are required for another application, you can enter a different start port, thus creating a new range. To change the start port, configure the following option in the 'RTP' section.

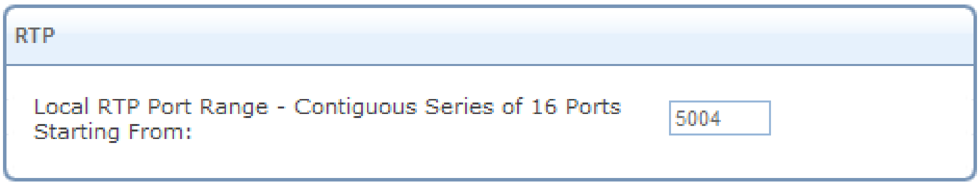


Figure 5.221 Advanced – RTP

Local RTP Port Range The range of ports reserved for Real Time Protocol (RTP) voice transport.

5.6.12.8 Configuring Quality of Service Parameters

Quality of Service (QoS) is aimed at improving the quality of voice traffic. To configure the QoS parameters, click the 'Advanced' link under the 'Voice' menu item. In the 'Quality of Service' section, configure the following options.

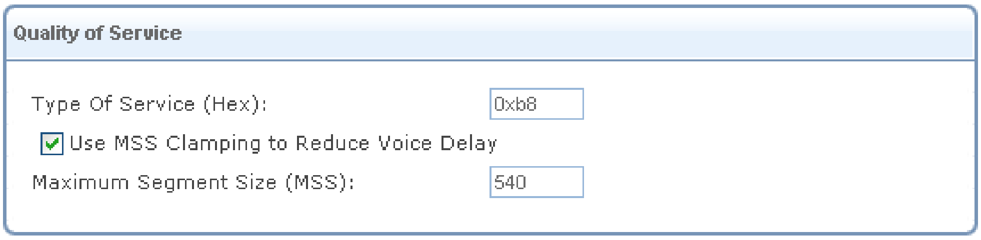


Figure 5.222 Advanced – Quality of Service

Type of Service (HEX) This is a part of the IP header that defines the type of routing service to be used to tag outgoing voice packets originated from OpenRG. It is used to tell routers along the way that this packet should get specific QoS. Leave this value as 0XB8 (default) if you are unfamiliar with the Differentiated Services IP protocol parameter.

Use MSS Clamping to Reduce Voice Delay When using Maximum Segment Size (MSS) Clamping, TCP streams routed via OpenRG when a voice call is active, will have a smaller segment size. This will cause RTP to receive better priority, and will help prevent high voice jitter that is caused by slow upstream transmission rate, which is common with most WAN connections (DSL, DOCSIS, etc.). When checking this option, the 'Maximum Segment Size (MSS)' field appears, where you can change the maximal segment size.

5.6.12.9 Configuring Dial Codes for Call Features

The 'Feature Codes' section enables you to view and customize activation codes for various call forwarding features.

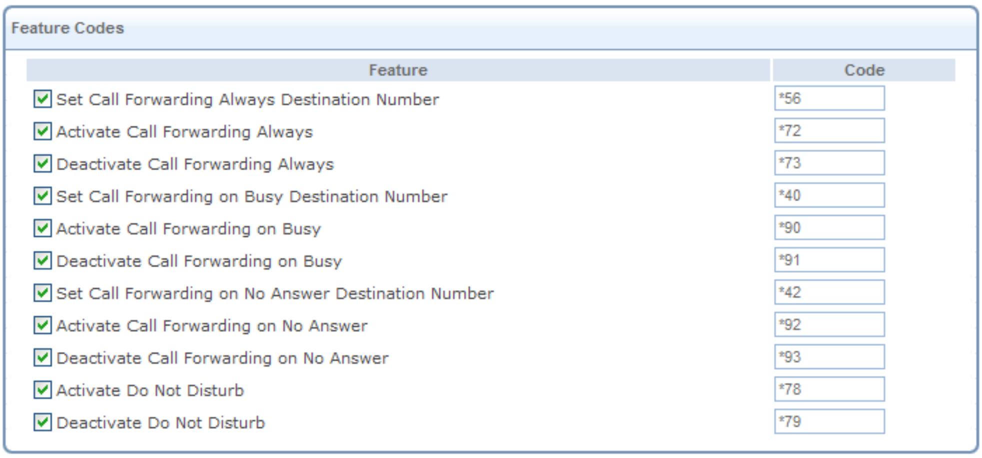


Figure 5.223 Feature Codes

Set Call Forwarding Always Destination Number Enables you to set an alternate destination number for all incoming calls, by entering **<extension number>#** after the feature's

code (*56 by default). For example, to set extension 300 as a destination number, dial *56300#. You will hear a voice confirmation for setting a destination number.

Activate Call Forwarding Always Forwards all incoming calls to a predefined extension. If you have not dialed a destination number when configuring the previous setting, a voice message will notify you accordingly. In this case, set a destination number as described earlier, prior to enabling the 'Activate Call Forwarding Always' feature. After dialing the code (*72 by default), you will hear a voice confirmation for the feature's activation.

Deactivate Call Forwarding Always Deactivates the 'Call Forwarding Always' feature. After dialing the code (*73 by default), you will hear a voice confirmation for 'Call Forwarding Always' deactivation.

Set Call Forwarding on Busy Destination Number Enables you to set an alternate destination for incoming calls, which are directed to a busy extension. After dialing the code (*40 by default), enter an extension number followed by "#". After dialing this sequence, you will hear a voice confirmation for setting the destination number.

Activate Call Forwarding on Busy Redirects a caller to an alternate extension, whenever the original target extension is busy. If you have not dialed a destination number when configuring the previous setting, a voice message will notify you accordingly. In this case, set a destination number as described earlier, prior to enabling the 'Call Forwarding on Busy' feature. After dialing the code (*90 by default), you will hear a voice confirmation for the feature's activation. Note that this feature is relevant only if the 'Call Forwarding Always' feature is deactivated.

Deactivate Call Forwarding on Busy Deactivates the 'Call Forwarding on Busy' feature. After dialing the feature's code (*91 by default), you will hear a voice confirmation for 'Call Forwarding on Busy' deactivation.

Set Call Forwarding on No Answer Destination Number Enables you to set an alternate destination number for incoming calls directed to an extension, which does not answer within a specific timeframe (by default, 20 seconds). Dial a destination number as described earlier, after the feature's code (*42 by default). You will hear a voice confirmation for setting the destination number.

Activate Call Forwarding on No Answer Redirects a caller to a alternate extension, whenever the original target extension does not answer within a specific timeframe. If you have not dialed a destination number when configuring the previous setting, a voice message will notify you accordingly. In this case, set a destination number as described earlier, prior to enabling the 'Call Forwarding on No Answer' feature. After dialing the code (*92 by default), you will hear a voice confirmation for the feature's activation. Note that this feature is relevant only if the 'Call Forwarding Always' feature is deactivated.

Deactivate Call Forwarding on No Answer Deactivates the 'Call Forwarding on No Answer' feature. After dialing the feature's code (*93 by default), you will hear a voice confirmation for 'Call Forwarding on No Answer' deactivation.

Activate Do Not Disturb Prevents calls from reaching a target extension. The caller will be forwarded to the extension's voice mail. After dialing the feature's code (*78 by default), you will hear a voice confirmation for the feature's activation.

Deactivate Do Not Disturb Cancels redirection of callers to the voice mail, and makes the target extension available for incoming calls. After dialing the feature's code (*79 by default), you will hear a voice confirmation for the feature's deactivation.

> Note: You can forward calls to external numbers by including an appropriate prefix. For example, if the prefix for external calls is '9', then by dialing *5691800555555#, you can forward calls to 1-800-555-555.

If either 'Call Forwarding Always' or 'Do Not Disturb' is activated, you will hear a stutter dial tone when picking up a phone connected to an analog extension.

5.6.12.10 Improving Voice Reception with Echo Cancellation

Echo cancellation is the elimination of reflected signals (echoes) made noticeable by delay in the network. This also improves the bandwidth of the line. When the delay of a voice call exceeds acceptable limits, OpenRG will protect the far end from receiving any echo generated at the local end and sent back through the network.

> Note: This feature is currently available on the following platforms: Intel IXP425, Broadcom BCM96358, and on platforms with the VINETIC chipset.

To improve voice reception with echo cancellation, click the 'Advanced' link under the 'Voice' item menu. In the 'Echo Cancellation' section, configure the following options.

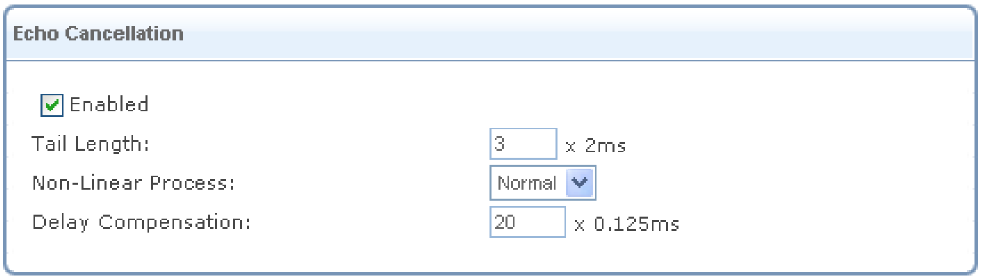


Figure 5.224 Advanced – Echo Cancellation

Enabled Select or deselect this check box to enable or disable this feature.

Tail Length Defines the length of the elapsed time frame used for calculating the extrapolation of the echo cancellation. A long tail improves the echo cancellation, but increases the load on the Digital Signal Processor (DSP).

Non-Linear Process (NLP) Determines the type of calculation that is used for removing the echo effect. You can set this feature to Normal, High or Off. Using high NLP improves the echo cancellation, but increases the load on the DSP.

Delay Compensation A time delay compensating the echo cancellation.

> Note: On some platforms, the feature's graphic interface may differ from the one presented in the above figure.

5.6.12.11 Saving Bandwidth with Silence Suppression

Silence suppression enables optimization when no speech is detected. With this feature enabled, OpenRG is able to detect the absence of audio and conserve bandwidth by preventing the transmission of "silent packets" over the network.

To save bandwidth with silence suppression, click the 'Advanced' link under the 'Voice' item menu. In the 'Silence Suppression' section, configure the following options.

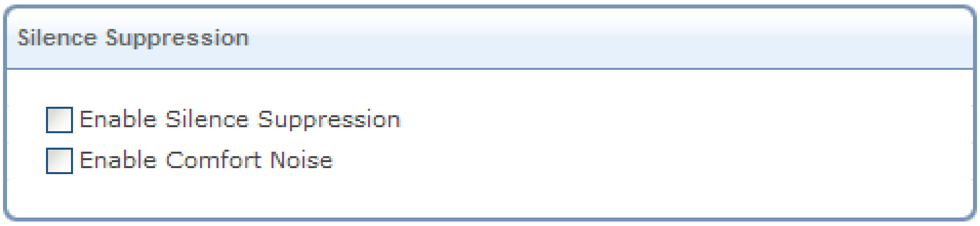


Figure 5.225 Advanced – Silence Suppression

Enable Silence Suppression Select this check box to enable this feature.

Enable Comfort Noise Select this option to play a soft "comfort" noise if the other side is performing silence suppression, in order to signal your caller that the conversation is still active.

5.6.12.12 Avoiding Voice Distortion with Jitter Buffer

A Jitter Buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in evenly spaced intervals. Variations in packet arrival time, called "jitter", can occur because of network congestion, timing drift, or route changes. The jitter buffer intentionally delays the arriving packets so that the end user experiences a clear connection with very little voice distortion.

To avoid voice distortion with jitter buffer, click the 'Advanced' link under the 'Voice' item menu. In the 'Jitter Buffer' section, configure the following options.

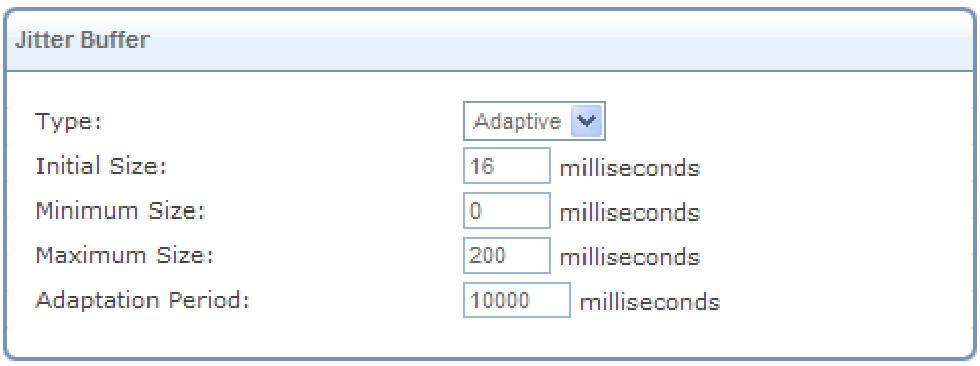


Figure 5.226 Advanced – Jitter Buffer

Type The type of the jitter buffer. Can be either adaptive or fixed. In case of adaptive jitter buffer, the following fields are visible:

Adapt According to Determines whether the jitter buffer size depends on the packet length or on the estimated network jitter.

Scaling Factor The size of the jitter buffer is Scaling Factor multiplied by packet length or by estimated network jitter (depending on the value of the previous field).

Local Adaptation The jitter buffer modifies its size during silence gaps. This way the change in delay is not noticed by the listener. This parameter determines when to perform this adaptation. The options are:

Off Regard as silence packets only those packets that the far end has marked as such.

On Regard as silence packets both the packets that the far end detected, and the packets that were locally detected as speech gaps.

On with sample interpolation No silence is needed. The adaptation is performed gradually through interpolation, so the listener does not notice the jitter buffer change in size. Notice that for this mode, modem or fax transmission could be distorted. This feature should only be used in the case of voice transmission.

Initial Size The initial size of the jitter buffer (in milliseconds).

Maximum Size The maximum size of the jitter buffer (in milliseconds).

Minimum Size The minimum size of the jitter buffer (in milliseconds).

5.6.12.13 Changing the FXS Ports Settings

The 'FXS Ports' section in the 'Advanced' screen contains advanced electronic settings for the FXS (analog) ports, which should only be modified by an experienced administrator or technician.

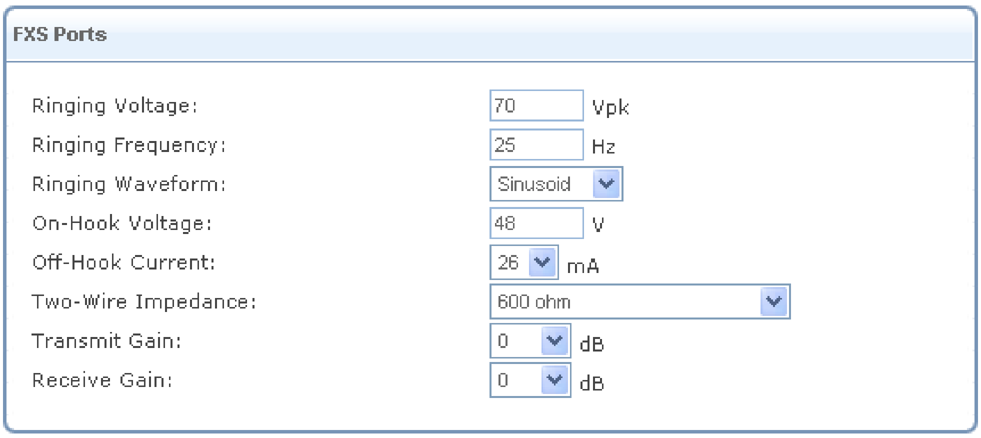


Figure 5.227 Advanced – FXS Ports

Ringing Voltage The ringing voltage in volts.

Ringing Frequency The ringing frequency in hertz.

Ringing Waveform The ringing waveform – sinusoid or trapezoid.

On-Hook Voltage The voltage of an idle handset in volts.

Off-Hook Current Limit The current of an active handset in milli-amperes.

Two-Wire Impedance Select the voice band impedance in ohms, synthesized by the SLIC.

Transmit Gain The transmit gain in decibels.

Receive Gain The receive gain in decibels.

5.6.12.14 Enable Voice

This section allows you to enable or disable OpenRG's Voice module.

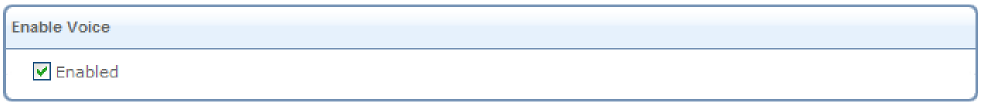


Figure 5.228 Enable Voice

Note: This feature is only available on gateways with the Asterisk-based Voice module.

To disable the Voice module, deselect the 'Enable Voice' check box, and click 'Apply'. The following message appears in all of the service's configuration screens.

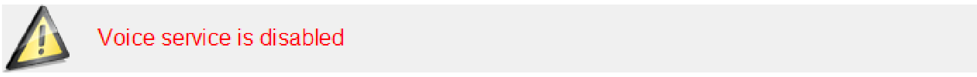


Figure 5.229 Disabled Voice Service

5.6.12.15 Configuring On Hook Caller ID Generation

The following settings determine the method by which the caller identity is generated while the handset is on-hook—the telephone is not in use.

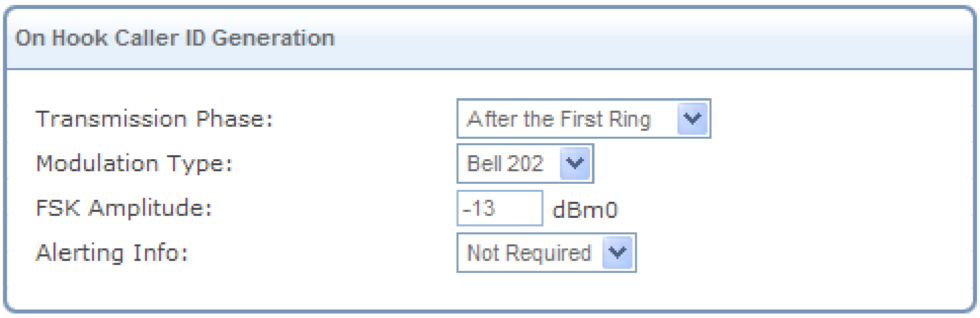


Figure 5.230 Advanced – On Hook Caller ID Generation

Transmission Phase Select when to display the caller ID—either before or after the first ring.

Modulation Type Select the modulation type—Bell 202 or ITU V.23.

FSK Amplitude Enter the Frequency Shift Keying amplitude.

Alerting Info Select DT-AS if alerting information is required. Otherwise, leave as "Not Required".

5.6.12.16 Configuring Off Hook Caller ID Generation

The following settings determine the method by which the caller identity is generated while the handset is off-hook—a conversation is active.

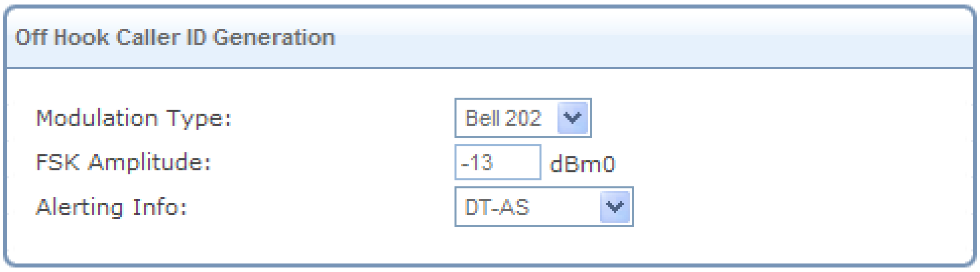


Figure 5.231 Advanced – Off Hook Caller ID Generation

Modulation Type Select the modulation type—Bell 202 or ITU V.23.

FSK Amplitude Enter the Frequency Shift Keying amplitude.

Alerting Info Select DT-AS if alerting information is required. Otherwise, leave as "Not Required".

5.6.12.17 Setting the Flash Button Timeout

The PBX distinguishes between pressing the hook and "Flash" button by the length of time that the Flash button is pressed. If it is pressed for longer than this timeframe, pressing Flash becomes equivalent to pressing the hook (phone hang-up).

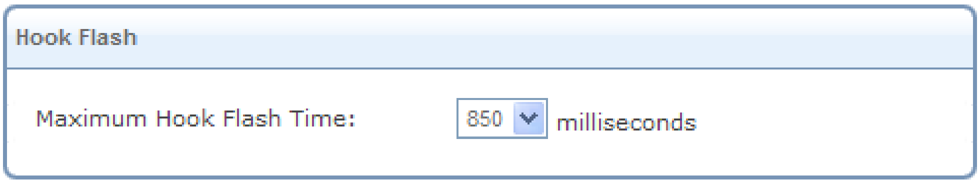


Figure 5.232 Advanced – Hook Flash

Maximum Hook Flash Time Select the maximum timeframe (between 250 and 850 milliseconds) after which pressing the Flash button hangs up the call.

5.7 Parental Control

The abundance of harmful information on the Internet is posing a serious challenge for employers and parents alike - "How can I regulate what my employee/child does on the net?"

OpenRG's Web-filtering allows parents and employers to regulate, control and monitor Internet access. By classifying and categorizing online content, it is possible to create numerous Internet access policies, and easily apply them to your home network computers. As a result, you may keep your children from harm's way by limiting access to adult and violent material, or increase employee productivity by regulating access to non work-related Internet content.

To effectively filter Web content one must first have a good idea of the kind of information that is available on the Internet. It is necessary to formulate a landscape of the accessible content, categorize and classify themes and subjects that may be considered inappropriate.

OpenRG's Parental Control categorization methodology provides an easy and straightforward method for fine-grained content filtering. The Parental Control module is constantly updated with URL-based information classified according to the following categories:

- Child protection
- Recreation and Entertainment
- Personal business
- Bandwidth control
- Advertisements
- Chat
- Remote Proxies and Hosting Sites (possibly untrusted sources)
- Other

Each category can be expanded into subcategories for better content control. For instance, the 'Recreation and Entertainment' category is comprised of subcategories such as:

- Arts and Entertainment
- Education
- Games
- Hobbies and Recreation

5.7.1 Overview

OpenRG's Parental Control service is provided by "Surf Control", a company specializing in Internet content filtering. Therefore, you must subscribe to this service in order to use this feature. You can subscribe through OpenRG's WBM, as described in the following section.

1. Under the 'Services; tab, click the 'Parental Control' menu item. The Parental Control's 'General' screen appears.

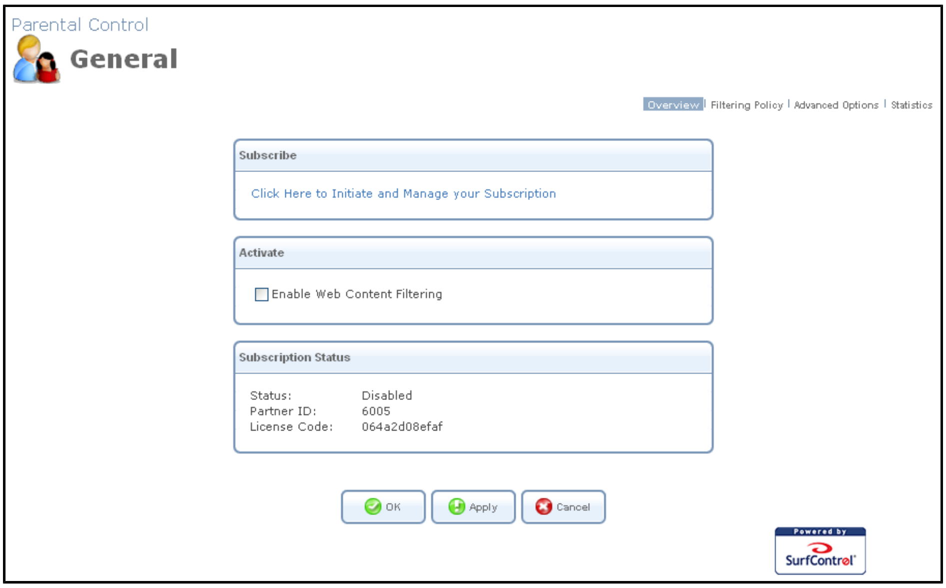


Figure 5.233 General

2. In the 'Activate' section, select the 'Enable Web Content Filtering' check box, and click 'Apply'. A 'Server Status' section is added.

3. If you have not subscribed yet or your subscription has expired, click the 'Click Here to Initiate and Manage your Subscription' link in the 'Subscribe' section. The Web filtering subscription site will then be displayed in a new browser window.

4. Follow the instructions on the site and subscribe for a free trial. You will be sent a verification email. Click the link in the verification email. Your subscription will be activated soon after clicking the verification link.

5. Return to OpenRG's WBM, and click the 'Parental Control' menu item under the 'Services' tab. The 'Filtering Policy' screen should be displayed with subscription expiry date at the top. If this is not the case, click the 'Advanced Options' link and then the 'Refresh Servers' button. Wait a few seconds and repeat this step.

5.7.2 Filtering Policy

5.7.2.1 Creating a Filtering Policy

A filtering policy defines which sites will be blocked based on their category. OpenRG provides four built-in policies:

Home Blocks sites under the 'Child Protection' category.

Employee Blocks sites from non work-related categories.

Block All Blocks all access to the Internet.

Allow All Allows unlimited Internet access.

These policies can be set from the 'Default Filtering Policy' drop-down menu in the 'Filtering Policy' screen (see Figure 5.234). To view or edit the 'Home' and 'Employee' policies, click their respective links in this screen. To create your own filtering policy, perform the following:

1. Click the 'Filtering Policy' link under the 'Parental Control' menu item. The 'Filtering Policy' screen appears.

Figure 5.234 Filtering Policy

2. Click the 'Add a policy' link. The following screen appears.

Figure 5.235 Creating a Filtering Policy

3. Enter a name and a description for the new policy.

4. Select the content filtering check boxes, which represent content you would like to block. Selecting a category will automatically select all its sub-categories and vice versa. If you would like to make a more refined selection of filtering options, click the plus sign (+) next to each category to display a list of its sub-categories. Note that clicking the minus sign (-) of a category will only be possible if all its sub-categories are either checked or unchecked.

5. You can also manually specify a list of Web sites and a list of URL keywords in the provided text fields, to which you can either block or allow access using the corresponding drop-down menu.

6. Click 'OK' to save the settings.

5.7.2.2 Applying the Filtering Policy

Once you have created different filtering policies, you can either define a default policy that will be applied to all of your LAN computers, or apply different policies to individual computers separately:

- LAN Filtering Policy – To select a default filtering policy for the LAN, select the policy name from the 'Default Filtering Policy' drop-down menu located in the 'Filtering Policy' screen (see Figure 5.234), and click Apply.

- PC Filtering Policy – To apply separate policies to individual home computers, perform the following:

  1. In the 'Filtering Policy' screen (see Figure 5.234), click the 'Add a LAN Computer' link. The 'LAN Computer Policy' screen appears.

Figure 5.236 LAN Computer Policy

  2. Enter the name or IP address of the LAN computer to which you wish to apply a policy.

  3. Select the policy you wish to apply in the 'Policy' drop-down menu.

  4. By default, the rule will always be active. However, you can define time segments during which the rule may be active, by selecting 'User Defined' from the 'Schedule' drop-down menu. If more than one scheduler rule is defined, the 'Schedule' drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

  5. Back in the 'Filtering Policy' screen, use the check box next to the computer name in order to enable or disable its policy.

  6. Click 'OK' to save the settings.

5.7.3 Advanced Options

Click the 'Advanced Options' link of the 'Parental Control' menu item under the 'Services' tab. The 'Advanced Options' screen appears.

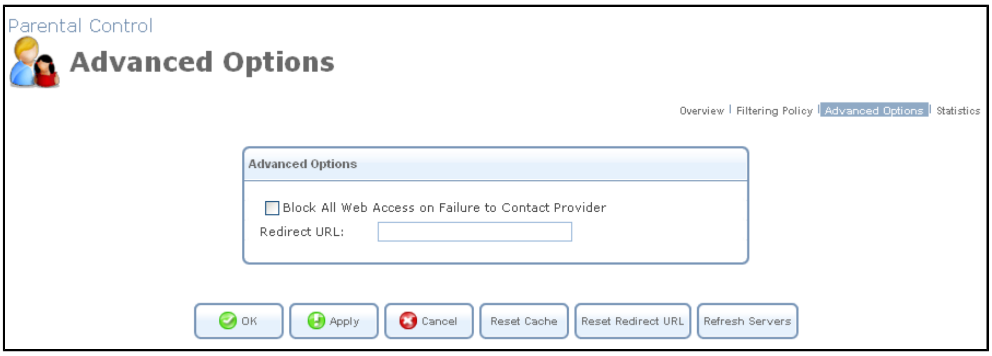


Figure 5.237 Advanced Options

Block All Web Access on Failure to Contact Provider The filtering service provider is consulted about every site's category in order to decide whether to allow or block it. If for any reason the provider cannot be consulted, use this check box to determine whether to block or allow access to all sites.

Redirect URL When a site is blocked, an OpenRG 'Blocked Access' page is displayed (see Figure 5.238), specifying the requested URL and the reason it was blocked. Use this field to specify an alternative page to be displayed when a site is blocked.

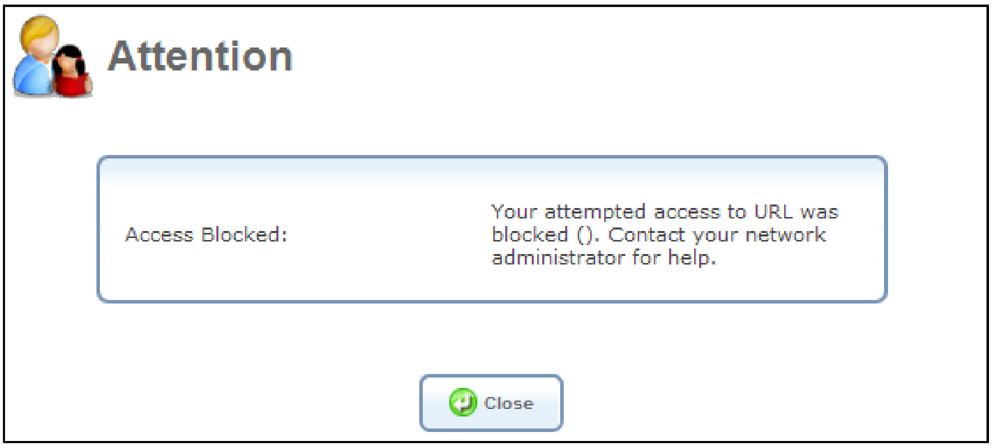


Figure 5.238 Blocked Access

5.7.4 Statistics

Click the 'Statistics' link of the 'Parental Control' menu item under the 'Services' tab. The 'Statistics' screen appears.

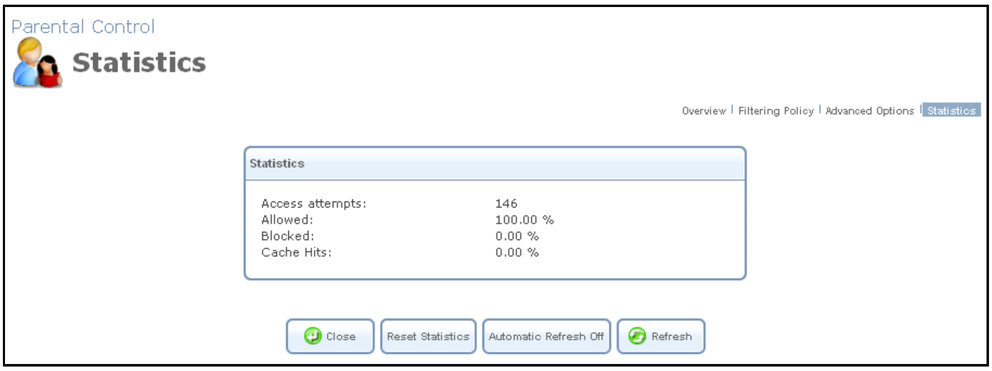


Figure 5.239 Statistics

The 'Statistics' screen monitors content filtering statistics. The statistics include a record of:

- Access attempts
- Allowed URLs
- Blocked URLs
- URLs that were accessed from Cache memory

Note: When Parental Control is enabled, HTTP services cannot be blocked by the 'Security Access Control' feature (refer to Section 5.2.2).

5.8 Virtual Private Network

5.8.1 Internet Protocol Security

Internet Protocol Security (IPSec) is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies procedures for securing private information transmitted over public networks. The IPSec protocols include:

- AH (Authentication Header) provides packet-level authentication.
- ESP (Encapsulating Security Payload) provides encryption and authentication.
- IKE (Internet Key Exchange) negotiates connection parameters, including keys, for the other two services.

Services supported by the IPSec protocols (AH, ESP) include confidentiality (encryption), authenticity (proof of sender), integrity (detection of data tampering), and replay protection (defense against unauthorized resending of data). IPSec also specifies methodologies for key management. Internet Key Exchange (IKE), the IPSec key management protocol, defines a series of steps to establish keys for encrypting and decrypting information; it defines a common language on which communications between two parties is based. Developed by the Internet

Engineering Task Force (IETF), IPSec and IKE together standardize the way data protection is performed, thus making it possible for security systems developed by different vendors to interoperate.

5.8.1.1 Technical Specifications

- Security architecture for the Internet Protocol
- IP Security Document Roadmap
- Connection type: Tunnel, Transport
- Use of Internet Security Association and Key Management Protocol (ISAKMP) in main and aggressive modes
- Key management: Manual, Automatic (Internet Key Exchange)
- NAT Traversal Negotiation for resolution of NATed tunnel endpoint scenarios
- Dead Peer Detection for tunnel disconnection in case the remote endpoint ceases to operate
- Gateway authentication: X.509, RSA signatures and pre-shared secret key
- IP protocols: ESP, AH
- Encryption: AES, 3DES, DES, NULL, HW encryption integration (platform dependent)
- Authentication: MD5, SHA-1
- IP Payload compression
- Interoperability: VPNC Certified IPSec, Windows 2000, Windows NT, FreeS/WAN, FreeBSD, Checkpoint Firewall-1, Safenet SoftRemote, NetScreen, SSH Sentinel

5.8.1.2 IPSec Settings

Access this feature either from the 'VPN' menu item under the 'Services' tab, or by clicking its icon in the 'Advanced' screen. The 'Internet Protocol Security (IPSec)' screen appears.

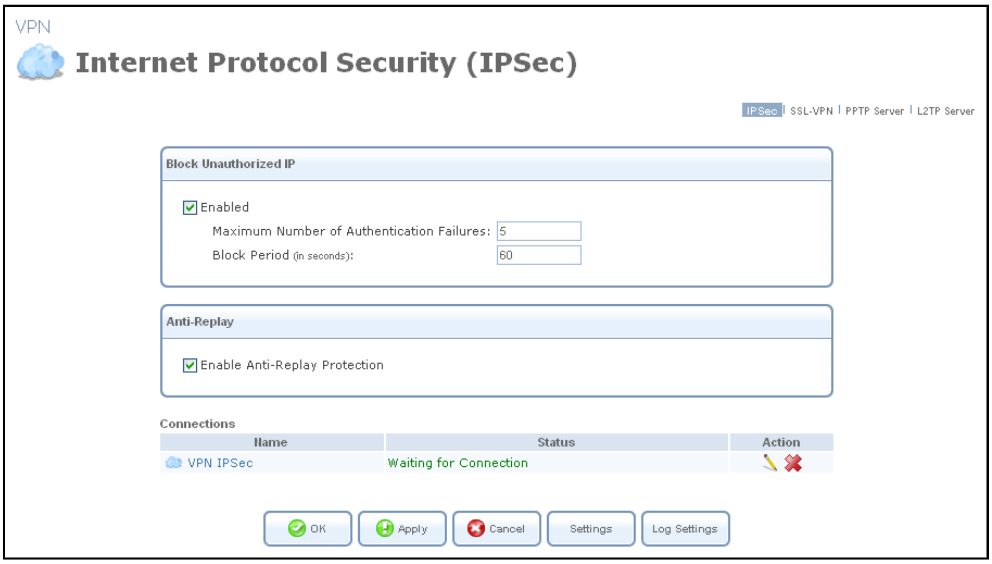


Figure 5.240 Internet Protocol Security (IPSec)

This screen enables you to configure the following settings:

Block Unauthorized IP Select the 'Enabled' check box to block unauthorized IP packets to OpenRG. Specify the following parameters:

- **Maximum Number of Authentication Failures** The maximum number of packets to authenticate before blocking the origin's IP address.
- **Block Period (in seconds)** The timeframe during which OpenRG will drop packets from an unauthorized IP address.

Enable Anti-Replay Protection Select this option to enable dropping of packets that are recognized (by their sequence number) as already been received.

Connections This section displays the list of IPSec connections. To learn how to create an IPSec connection, refer to Section 6.4.13.

5.8.1.2.1 Public Key Management

The 'Settings' button in the 'Internet Protocol Security (IPSec)' screen enables you to manage OpenRG's public keys.

1. Click the 'Settings' button (see Figure 5.240) to view OpenRG's public key. If necessary, you can copy the public key from the screen that appears.

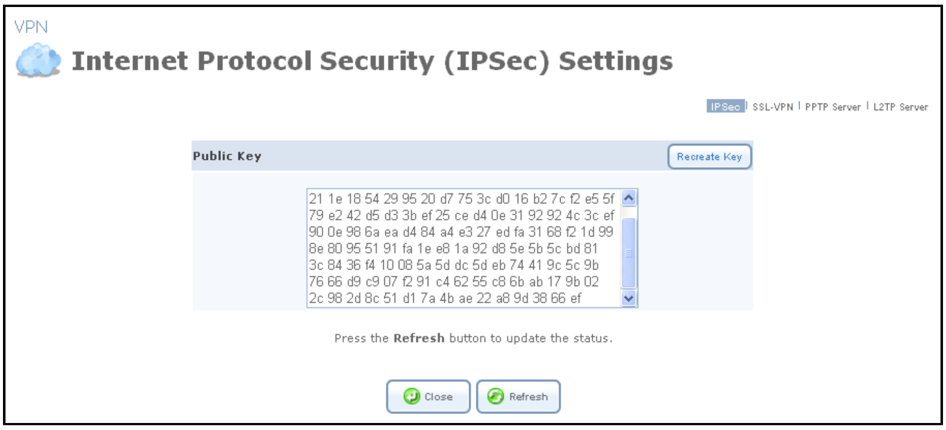


Figure 5.241 Internet Protocol Security (IPSec) Settings

2. Click the 'Recreate Key' button to recreate the public key, or the 'Refresh' button to refresh the key displayed in this screen.

5.8.1.2.2 Log Settings

The IPSec Log can be used to identify and analyze the history of the IPSec package commands, attempts to create connections, etc. The IPSec activity, as well as that of other OpenRG modules, are displayed together in this view.

1. Click the 'Log Settings' button. The 'IPSec Log Settings' screen appears (see Figure 5.242).
2. Select the check boxes relevant to the information you would like the IPSec log to record.
3. Click 'OK' to save the settings.

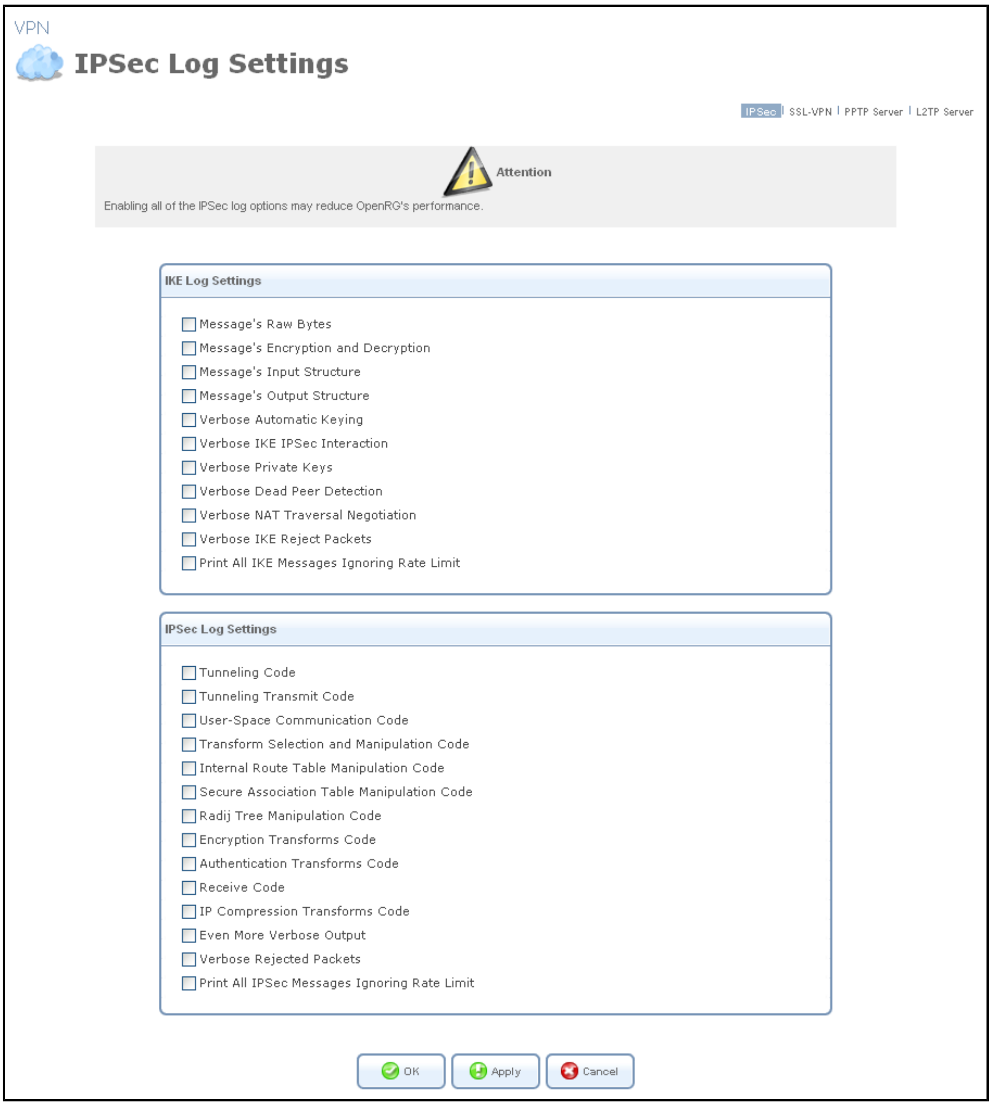


Figure 5.242 IPSec Log Settings

5.8.1.3 IPSec Connection Settings

The IPSec connections are displayed under the 'Connections' section of the 'Internet Protocol Security (IPSec)' screen (see Figure 5.240), in addition to the general 'Network Connections' screen (refer to Section 6.4). To configure an IPSec connection settings, perform the following:

1. Click the connection's action icon . The 'VPN IPSec Properties' screen appears, displaying the 'General' sub-tab.

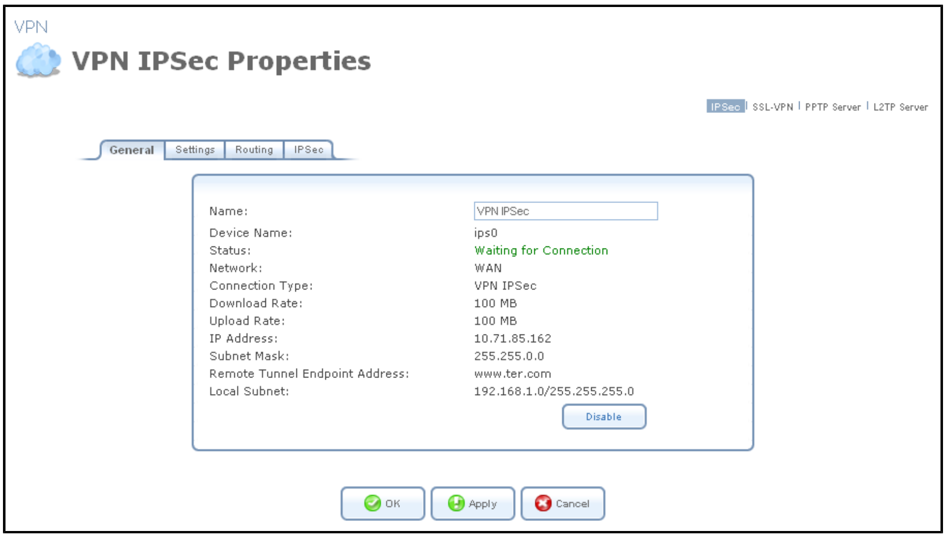


Figure 5.243 VPN IPSec Properties – General

2. Click the 'Settings' sub-tab, and configure the following settings:

Figure 5.244 VPN IPSec Properties – Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

3. Click the 'Routing' sub-tab, and define the connection's routing rules. To learn how to create routing rules, refer to Section 6.6.

Figure 5.245 VPN IPSec Properties – Routing

4. Click the 'IPSec' sub-tab, and configure the following settings.

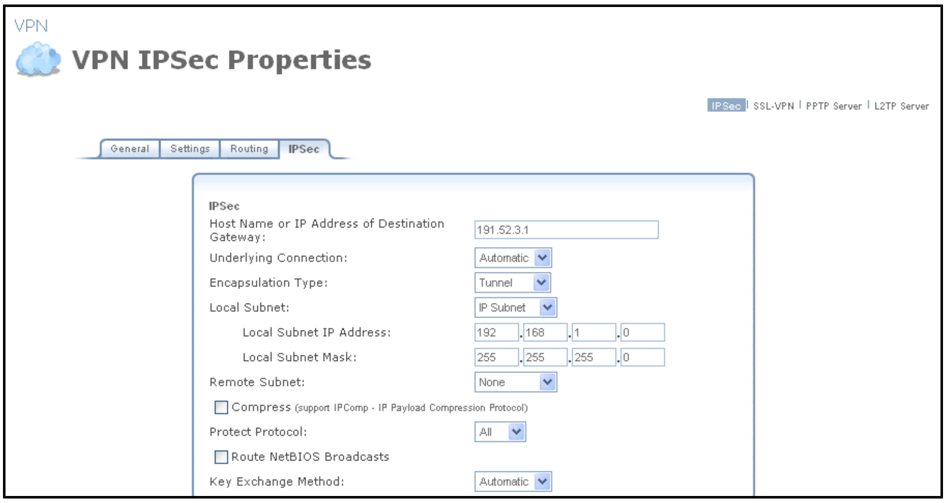


Figure 5.246 VPN IPSec Properties – IPSec

Host Name or IP Address of Destination Gateway The IP address of your IPSec peer. If your connection is an IPSec Server, this field will display "Any Remote Gateway".

Underlying Connection In a single WAN scenario, the underlying connection parameter will be set to "Automatic" (non-configurable). However, if you have multiple WAN devices, a drop-down menu will appear (see Figure 5.244), enabling you to choose the underlying WAN device. The IPSec connection will only use your chosen device, unless failover is enabled. In this case, the failed-to device will be used instead (assuming its route rules consent), until the chosen device is up again. Note that if you select "Automatic", there will be no attempt to return to the original device from the failed-to device. For more information about failover, refer to Section 6.6.1.3.3.

Encapsulation Type Select between 'Tunneling' or 'Transport' encapsulation. 'Transport' encapsulation is performed between two gateways (no subnets), and therefore needs no explicit configuration. 'Tunneling' requires that you configure the following parameters:

- **Local Subnet** Define your local endpoint, by selecting one of the following options:

IP Subnet (default) Enter OpenRG's Local Subnet IP Address and Local Subnet Mask.

IP Range Enter the 'From' and 'To' IP addresses, forming the endpoints range of the local subnet(s).

IP Address Enter the Local IP Address to define the endpoint as a single host.

None Select this option if you do not want to define a local endpoint. The endpoint will be set to the gateway.

- **Remote Subnet** This section is identical to the 'Local Subnet' section above, but is for defining the remote endpoint.

  Compress (Support IPComp protocol) Select this check box to compress packets during encapsulation with the IP Payload Compression protocol. Please note that this reduces performance (and is therefore unchecked by default).

Protect Protocol Select the protocols to protect with IPSec: All, TCP, UDP, ICMP or GRE. When selecting TCP or UDP, additional source port and destination port drop-down menus will appear, enabling you to select 'All' or to specify 'Single' ports in order to define the protection of specific packets. For example, in order to protect L2TP packets, select UDP and specify 1701 as both single source and single destination ports.

Route NetBIOS Broadcasts Select this option to allow NetBIOS packets through the IPSec tunnel, which otherwise would not meet the routing conditions specified.

Key Exchange Method The IPSec key exchange method can be 'Automatic' (the default) or 'Manual'. Selecting one of these options will alter the rest of the screen.

1. Automatic key exchange settings:

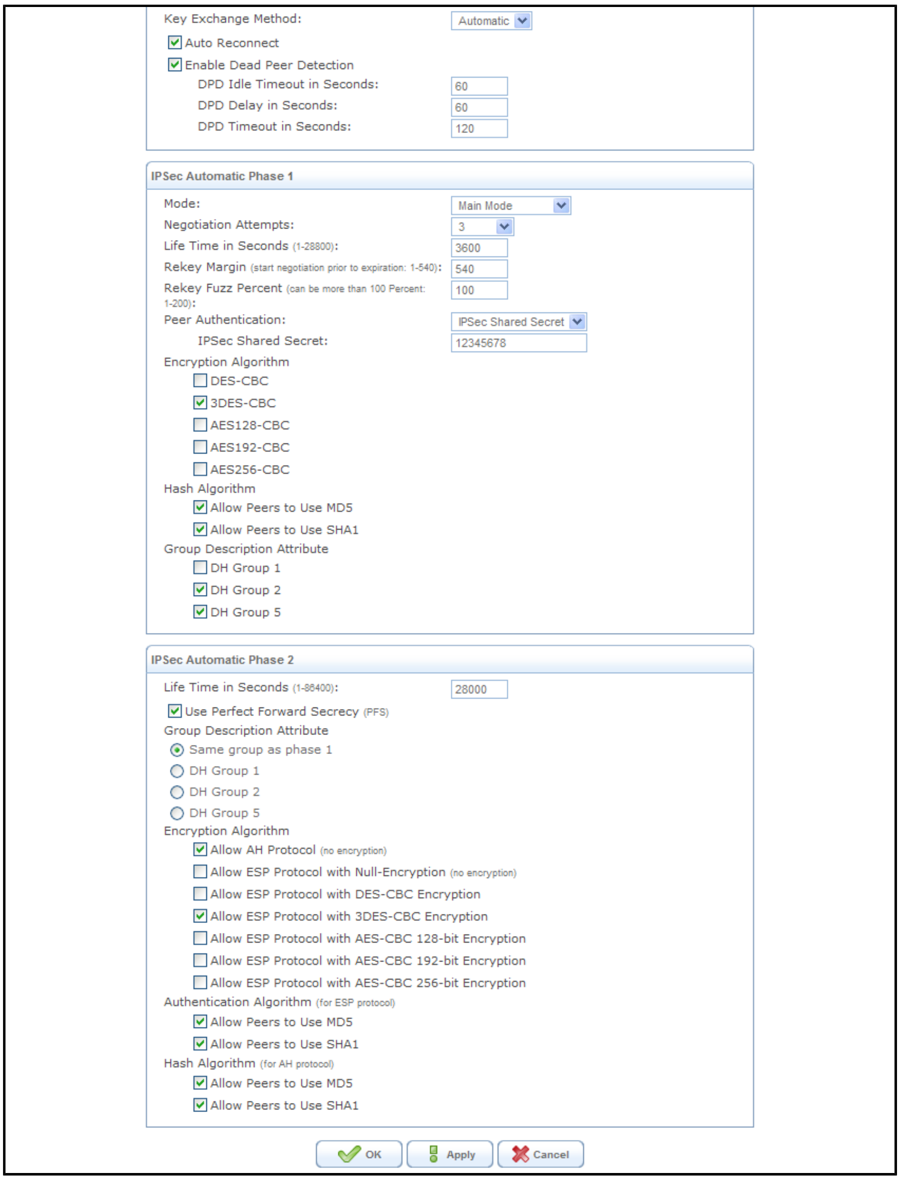


Figure 5.247 Automatic Key Exchange Settings

Auto Reconnect The IPSec connection will reconnect automatically if disconnected for any reason.

Enable Dead Peer Detection OpenRG will detect whether the tunnel endpoint has ceased to operate, in which case will terminate the connection. Note that this feature will be functional only if the other tunnel endpoint supports it. This is determined during the negotiation phase of the two endpoints.

- **DPD Idle Timeout in Seconds** Defines how long the IPSec tunnel can be idle before OpenRG sends the first DPD message to the remote peer, in order to check if it is alive.

- **DPD Delay in Seconds** Defines how long OpenRG will wait for the peer's response to the DPD message, before sending an additional message (in case of response failure).

- **DPD Timeout in Seconds** Defines how long OpenRG will try to contact the peer, before it declares the peer dead and terminates the connection.

IPSec Automatic Phase 1 – Peer Authentication

- **Mode** Select the IPSec mode – either 'Main Mode' or 'Aggressive Mode'. Main mode is a secured but slower mode, which presents negotiable propositions according to the authentication algorithms that you select in the check boxes. Aggressive Mode is faster but less secured. When selecting this mode, the algorithm check boxes are replaced by radio buttons, presenting strict propositions according to your selections.

- **Negotiation attempts** Select the number of negotiation attempts to be performed in the automatic key exchange method. If all attempts fail, OpenRG will wait for a negotiation request.

- **Life Time in Seconds** The timeframe in which the peer authentication will be valid.

- **Rekey Margin** Specifies how long before connection expiry should attempts to negotiate a replacement begin. It is similar to that of the key life time and is given as an integer denoting seconds.

- **Rekey Fuzz Percent** Specifies the maximum percentage by which Rekey Margin should be randomly increased to randomize re-keying intervals.

- **Peer Authentication** Select the method by which OpenRG will authenticate your IPSec peer.

  - **IPSec Shared Secret** – Enter the IPSec shared secret.

  - **RSA Signature** – Enter the peer's RSA signature (based on OpenRG's public key), as described in Section 5.8.1.5.3.

  - **Certificate** – If a certificate exists on OpenRG, it will appear when you select this option. Enter the certificate's local ID and peer ID. To learn how to add certificates to OpenRG, refer to Section 6.9.4.

- **Encryption Algorithm** Select the encryption algorithms that OpenRG will attempt to use when negotiating with the IPSec peer.

- **Hash Algorithm** Select the hash algorithms that OpenRG will attempt to use when negotiating with the IPSec peer.

- **Group Description Attribute** Select the Diffie-Hellman (DH) group description(s). Diffie-Hellman is a public-key cryptography scheme that allows two parties to establish a shared secret over an insecure communications channel.

IPSec Automatic Phase 2 – Key Definition

- **Life Time in Seconds** The length of time before a security association automatically performs renegotiation.
- **Use Perfect Forward Secrecy (PFS)** Select whether Perfect Forward Secrecy of keys is required on the connection's keying channel (with PFS, penetration of the key-exchange protocol does not compromise keys negotiated earlier). Deselecting this option will hide the next parameter.

  Group Description Attribute Select whether to use the same group chosen in phase 1, or reselect specific groups.
- **Encryption Algorithm** Select the encryption algorithms that OpenRG will attempt to use when negotiating with the IPSec peer.
- **Authentication Algorithm (for ESP protocol)** Select the authentication algorithms that OpenRG will attempt to use when negotiating with the IPSec peer.
- **Hash Algorithm (for AH protocol)** Select the hash algorithms that OpenRG will attempt to use when negotiating with the IPSec peer.

2. Manual key definition:

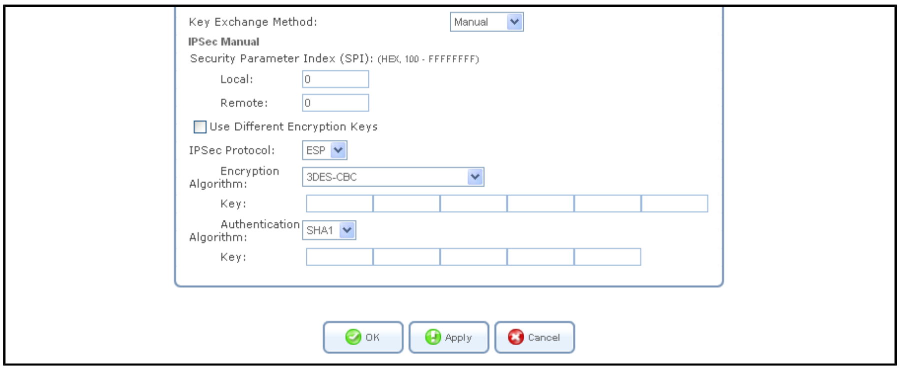


Figure 5.248 Manual Key Definition

Security Parameter Index (SPI): (HEX, 100 - FFFFFFFF) A 32 bit value that together with an IP address and a security protocol, uniquely identifies a particular security association. The local and remote values must be coordinated with their respective values on the IPSec peer.

Use Different Encryption Keys Selecting this option allows you to define both local and remote algorithm keys when defining the IPSec protocol (in the next section).

IPSec Protocol Select between the ESP and AH IPSec protocols. The screen will refresh accordingly:

- **ESP** – Select the encryption and authentication algorithms, and enter the algorithm keys in hexadecimal representation.

- **AH** – Select the hash algorithm, and enter the algorithm key in hexadecimal representation.

5. Click 'OK' to save the settings.

5.8.1.4 IPSec Gateway-to-Host Connection Scenario

In order to create an IPSec connection between OpenRG and a Windows host, you need to configure both the gateway and the host. This section describes both OpenRG's configuration and a Windows XP client configuration.

5.8.1.4.1 Configuring IPSec on OpenRG

1. Under the 'System' tab, click the 'Network Connections' menu item. The 'Network Connections' screen appears.

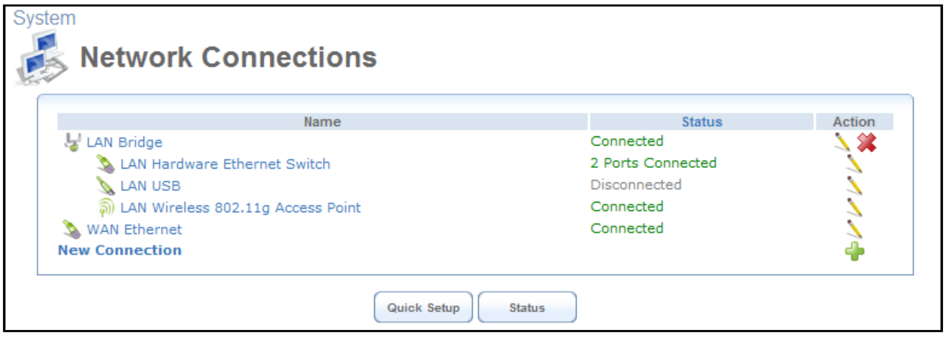


Figure 5.249 Network Connections

2. Click the 'New Connection' link. The 'Connection Wizard' screen appears.

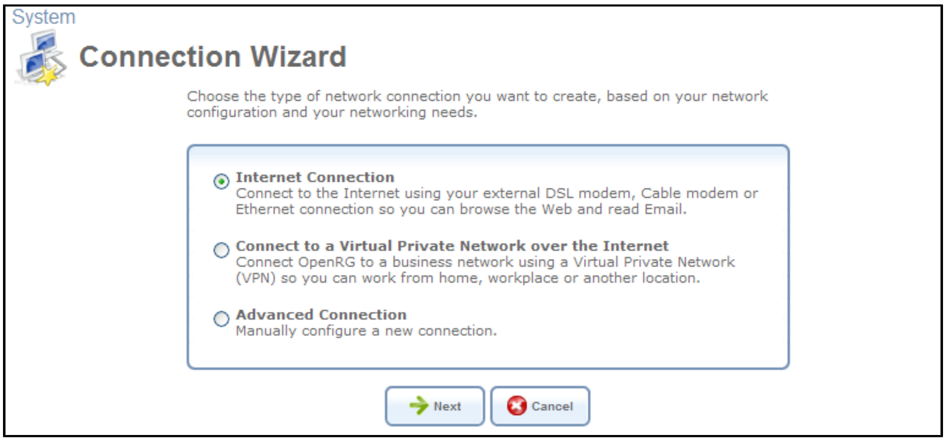


Figure 5.250 Connection Wizard

3. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears.

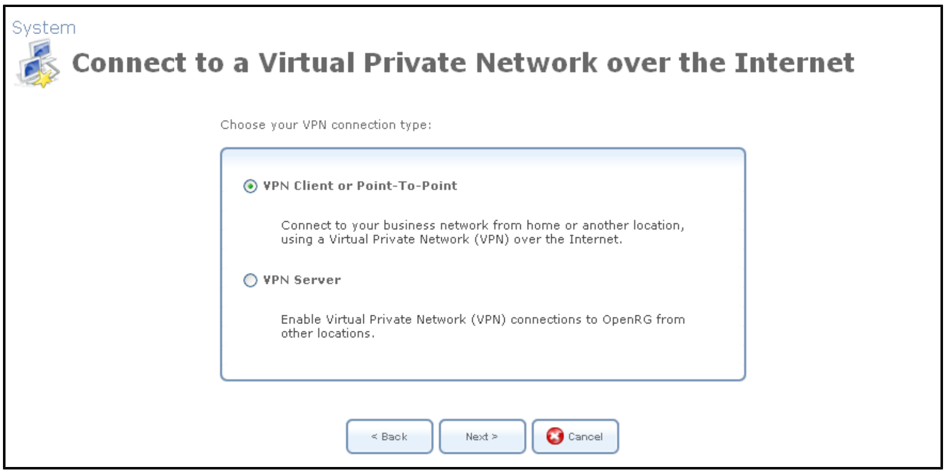


Figure 5.251 Connect to a Virtual Private Network over the Internet

4. Select the 'VPN Client or Point-To-Point' radio button and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

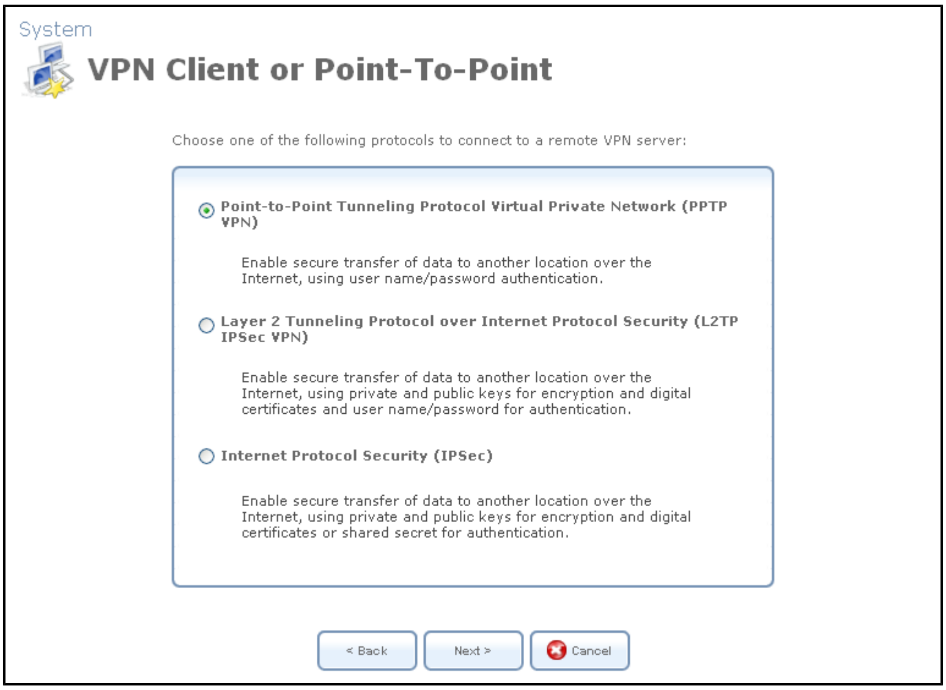


Figure 5.252 VPN Client or Point-To-Point

5. Select the 'Internet Protocol Security (IPSec)' radio button and click 'Next'. The 'Internet Protocol Security (IPSec)' screen appears.

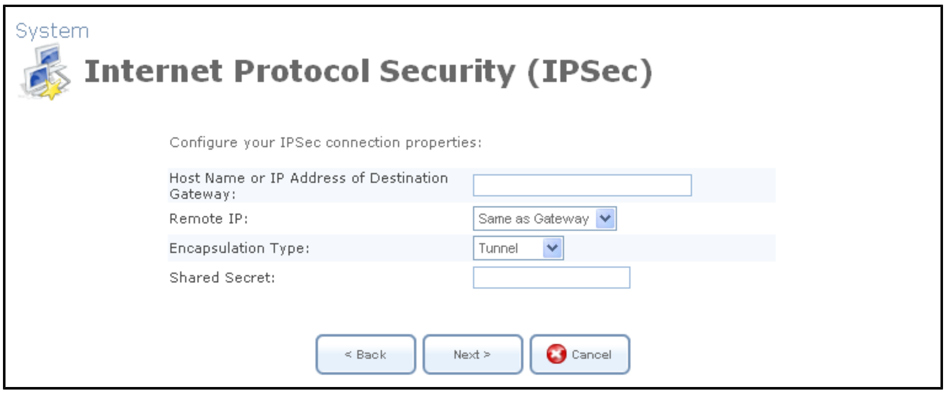


Figure 5.253 Internet Protocol Security (IPSec)

6. Specify the following parameters:

   Host Name or IP Address of Destination Gateway Specify 22.23.24.25

   Remote IP Select "Same as Gateway".

   Encapsulation Type Select "Tunnel".

   Shared Secret Enter "hr5x".

7. Click 'Next'. The 'Connection Summary' screen appears.

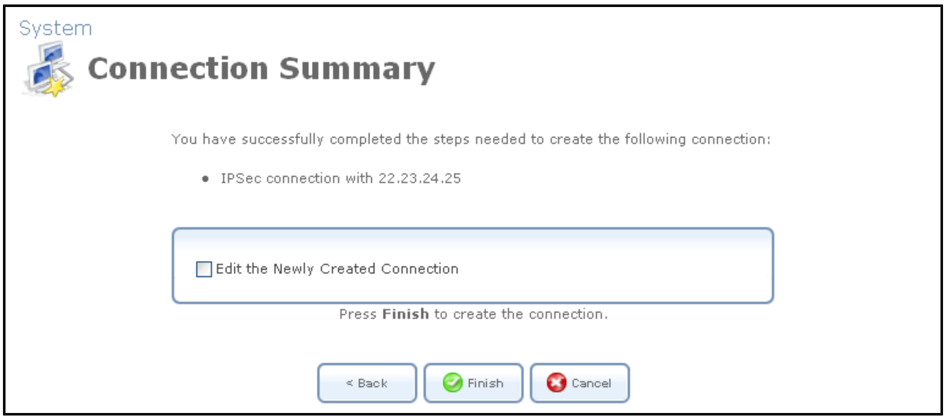


Figure 5.254 Connection Summary

8. Click 'Finish'. The 'Network Connections' screen displays the newly created IPSec connection.

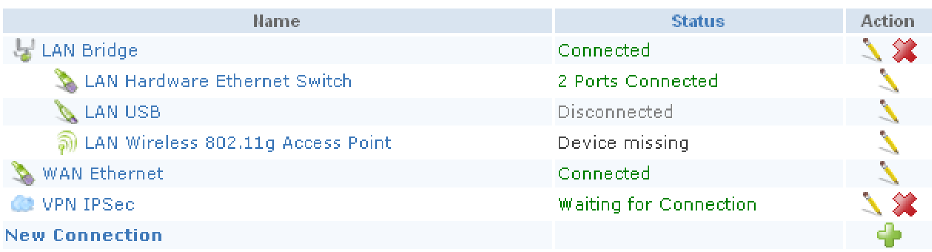


Figure 5.255 New VPN IPSec Connection

5.8.1.4.2 Configuring IPSec on the Windows Host

The following IP addresses are needed for the host configuration:

- Windows IP address – referred to as <windows_ip>.
- OpenRG WAN IP address – referred to as <openrg_wan_ip>.
- OpenRG LAN Subnet address – referred to as <openrg_lan_subnet>.

The configuration sequence:

1. Creating the IPSec Policy:

   a. Click the Start button and select Run. Type "secpol.msc" and click 'OK'. The 'Local Security Settings' window appears.

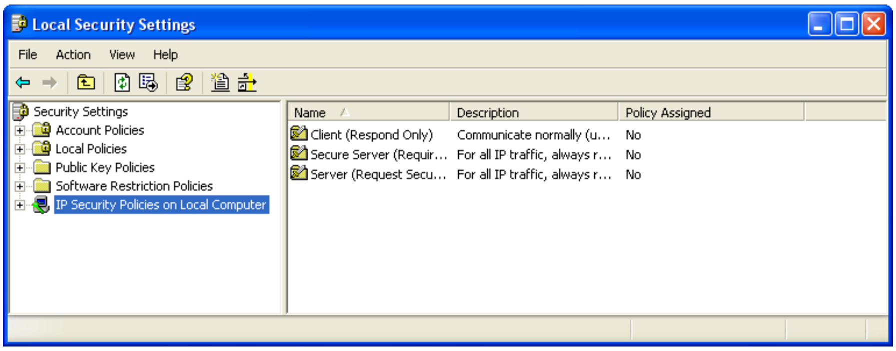


Figure 5.256 Local Security Settings

   b. Right-click the 'IP Security Policies on Local Computer' and choose 'Create IP Security Policy...'. The IP Security Policy Wizard appears.

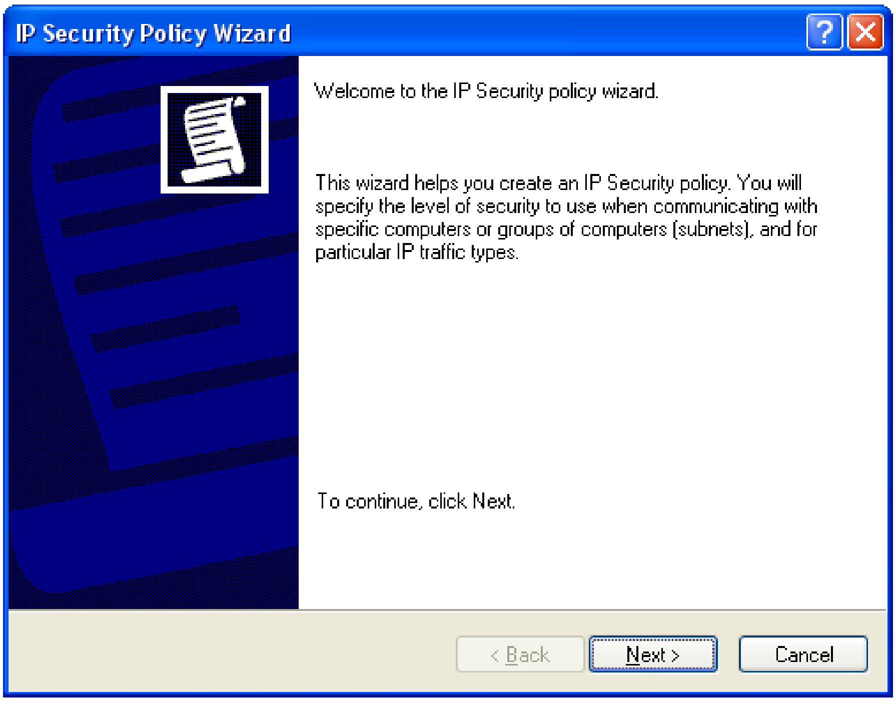


Figure 5.257 IP Security Policy Wizard

c. Click 'Next' and type a name for your policy, for example "OpenRG Connection".

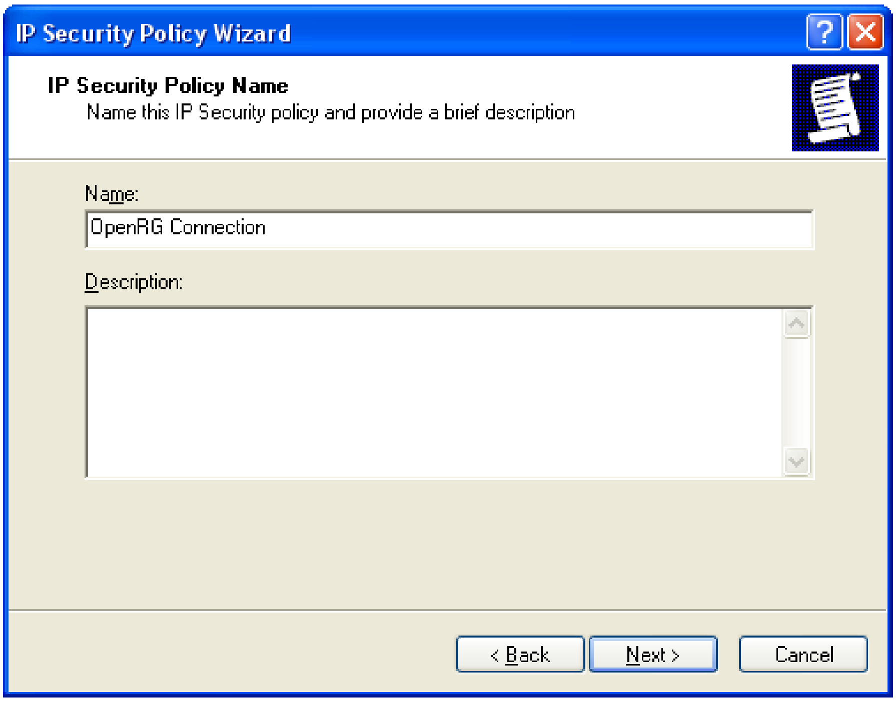


Figure 5.258 IP Security Policy Name

d. Click 'Next'. The 'Requests for Secure Communication' screen appears.

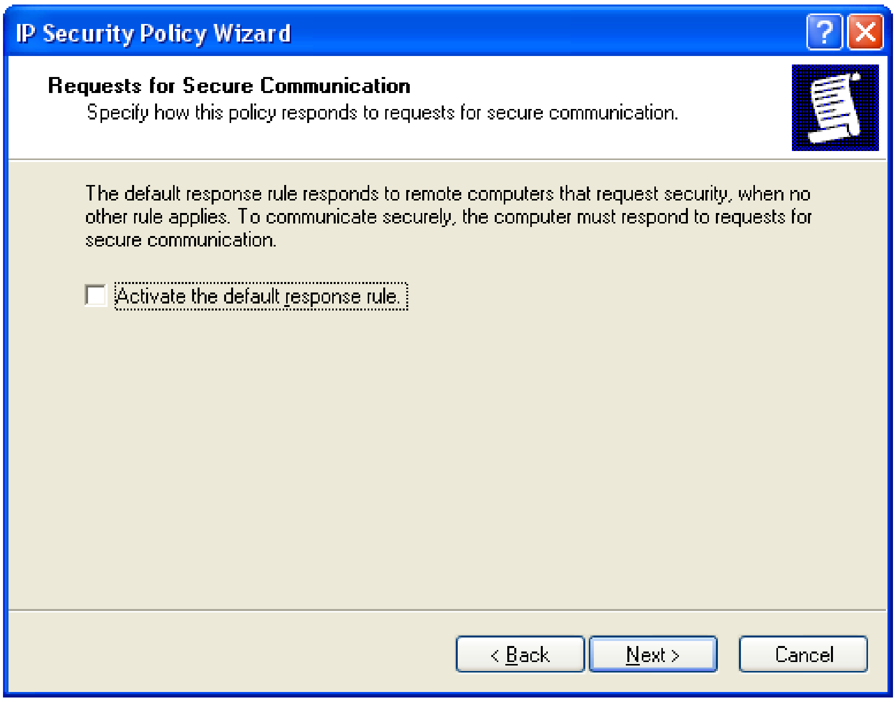


Figure 5.259 Requests for Secure Communication

e. Deselect the 'Activate the default response rule' check box, and click 'Next'. The 'Completing the IP Security Policy Wizard' screen appears.

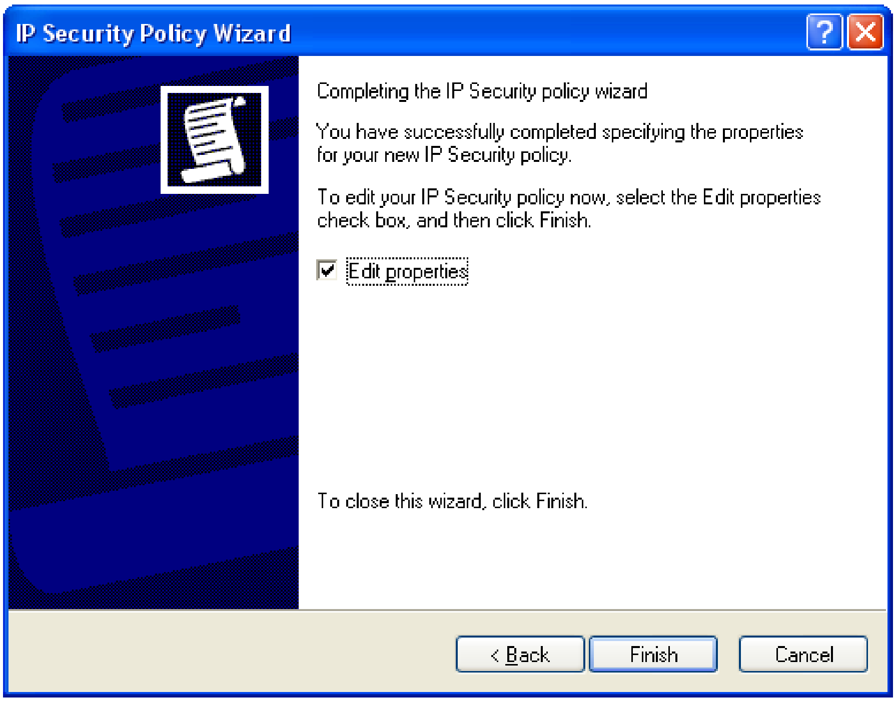


Figure 5.260 Completing the IP Security Policy Wizard

f. Make sure that the 'Edit Properties' check box is selected, and click 'Finish'. The 'OpenRG Connection Properties' window appears.

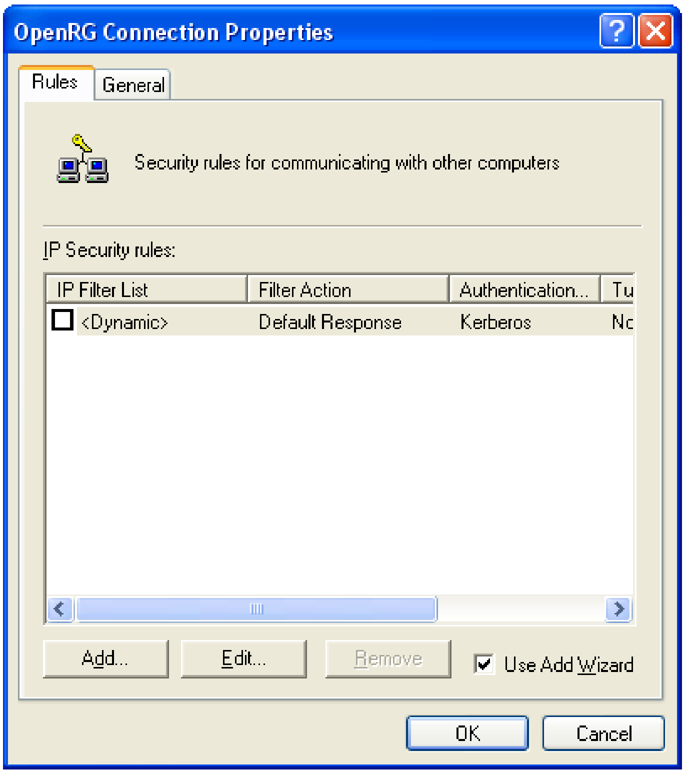


Figure 5.261 OpenRG Connection Properties

g. Click 'OK'.

2. Building Filter List 1 – Windows XP to OpenRG:

   a. In the 'Local Security Settings' window, right-click the new 'OpenRG Connection' policy, created in the previous step, and select Properties. The Properties window appears (see Figure 5.261).

   b. Deselect the 'Use Add Wizard' check box and click the 'Add' button to create a new IP Security rule. The 'New Rule Properties' window appears.

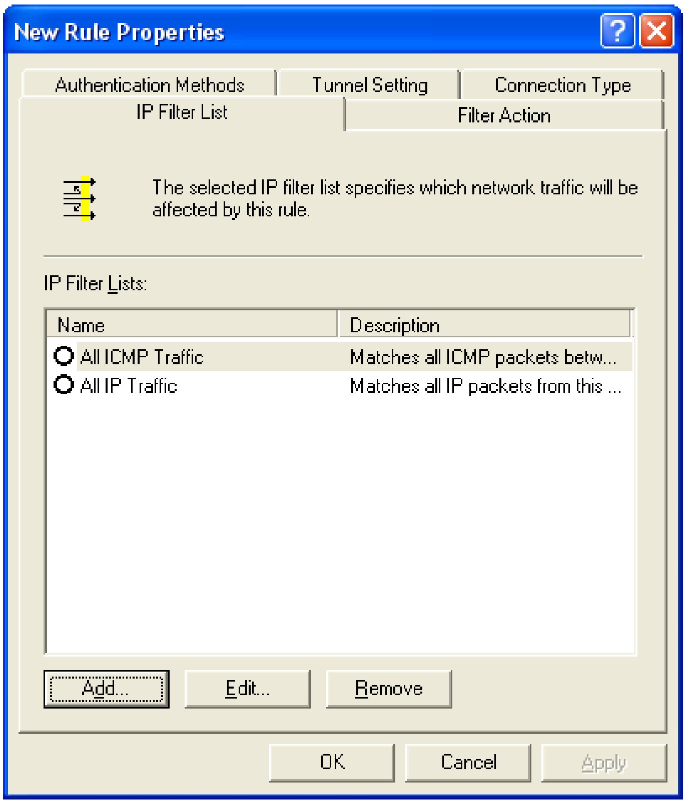


Figure 5.262 New Rule Properties

c. Under the IP Filter List tab, click the 'Add' button. The 'IP Filter List' window appears.

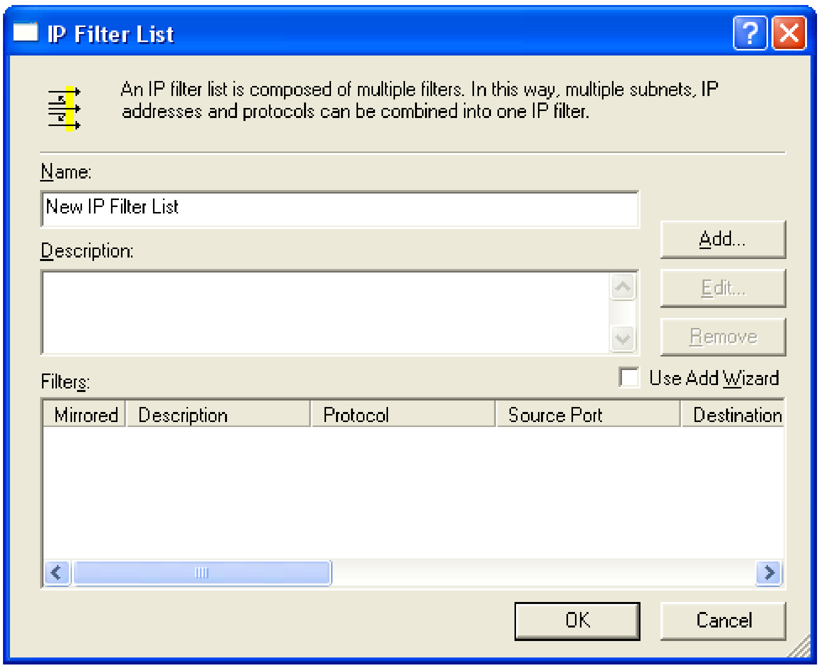


Figure 5.263 IP Filter List

d. Enter the name "Windows XP to OpenRG" for the filter list, and deselect the 'Use Add Wizard' check box. Then, click the 'Add' button. The 'Filter Properties' window appears.

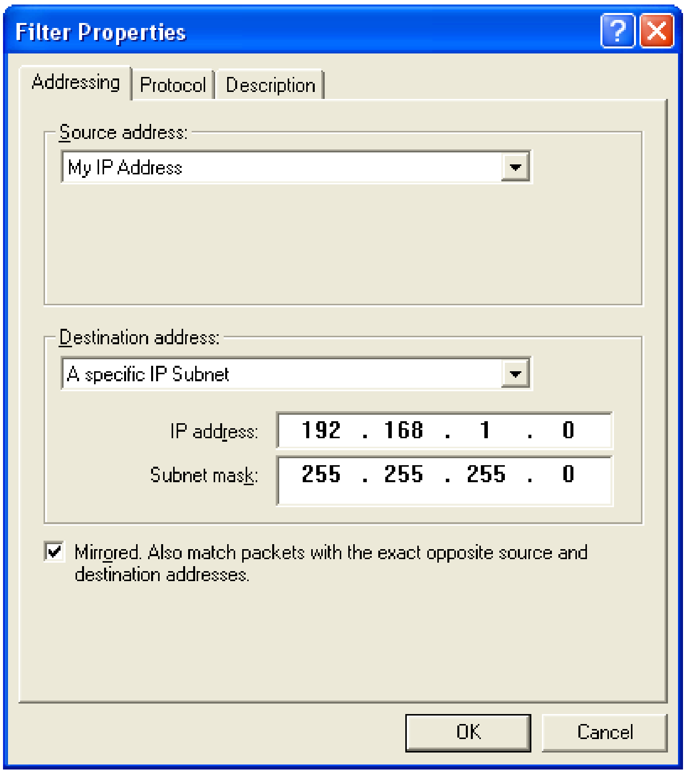


Figure 5.264 Filter Properties

e. In the 'Source address' drop-down menu, select 'My IP Address'.

f. In the 'Destination address' drop-down menu, select 'A Specific IP Subnet'. In the 'IP Address' field, enter the LAN Subnet (<openrg_lan_subnet>), and in the 'Subnet mask' field enter 255.255.255.0.

g. Click the 'Description' tab if you would like to enter a description for your filter.

h. Click the 'OK' button. Click 'OK' again in the 'IP Filter List' window to save the settings.

3. Building Filter List 2 – OpenRG to Windows XP:

   a. Under the IP Filter List tab of the 'New Rule Properties' window, click the 'Add' button. The 'IP Filter List' window appears (see Figure 5.263).

   b. Enter the name "OpenRG to Windows XP" for the filter list, deselect the 'Use Add Wizard' check box, and click the 'Add' button. The 'Filter Properties' window appears.

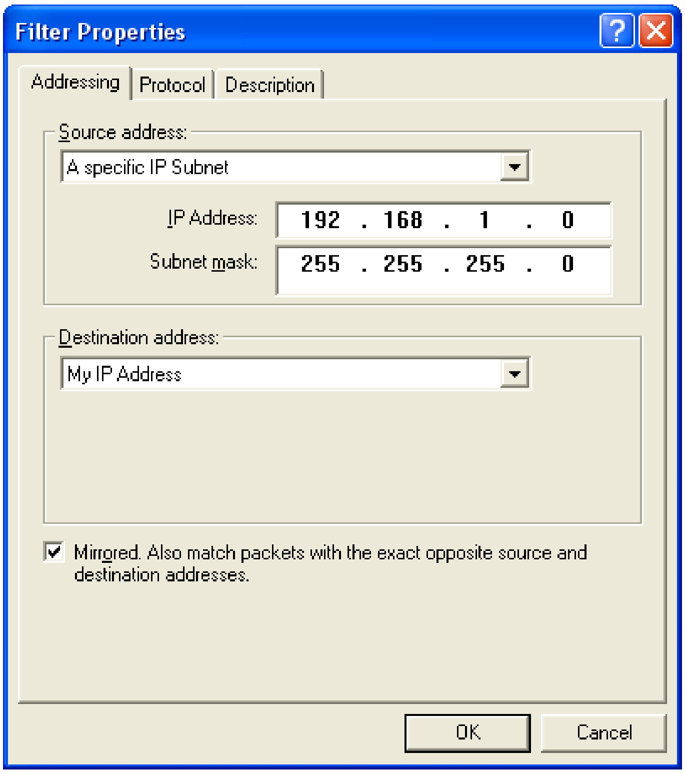


Figure 5.265 Filter Properties

c. In the 'Source address' drop-down menu, select 'A Specific IP Subnet'. In the 'IP Address' field enter the LAN Subnet (<openrg_lan_subnet>), and in the 'Subnet mask' field enter 255.255.255.0.

d. In the 'Destination address' drop-down menu, select 'My IP Address'.

e. Click the 'Description' tab if you would like to enter a description for your filter.

f. Click the 'OK' button. Click 'OK' again in the 'IP Filter List' window to save the settings.

4. Configuring Individual Rule of Tunnel 1 (Windows XP to OpenRG):

   a. Under the 'IP Filter List' tab of the 'New Rule Properties' window, select the 'Windows XP to OpenRG' radio button.

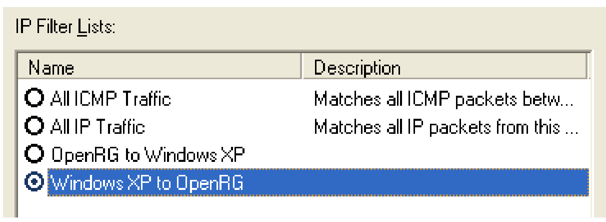


Figure 5.266 IP Filter List

   b. Click the 'Filter Action' tab.

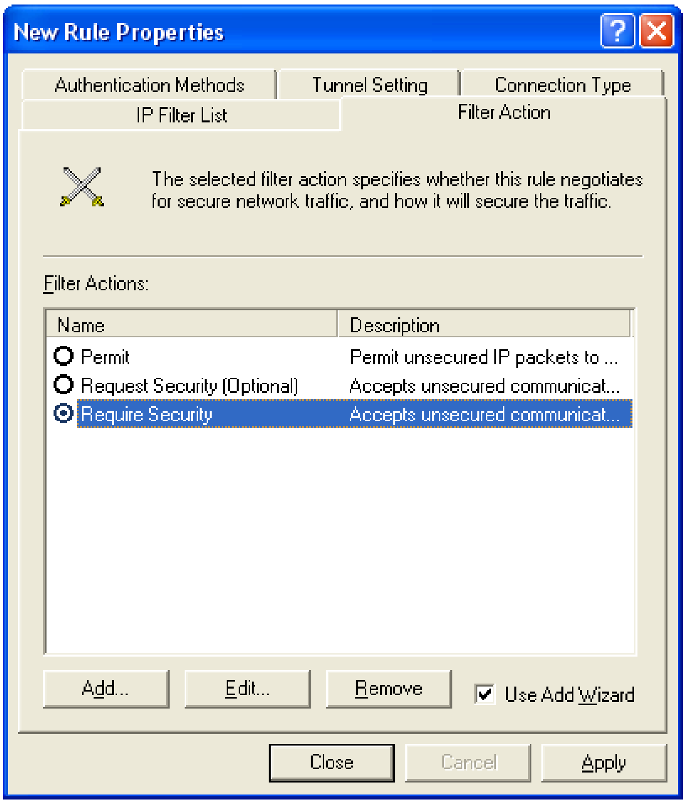


Figure 5.267 Filter Action

c. Select the 'Require Security' radio button, and click the 'Edit' button. The 'Require Security Properties' window appears.

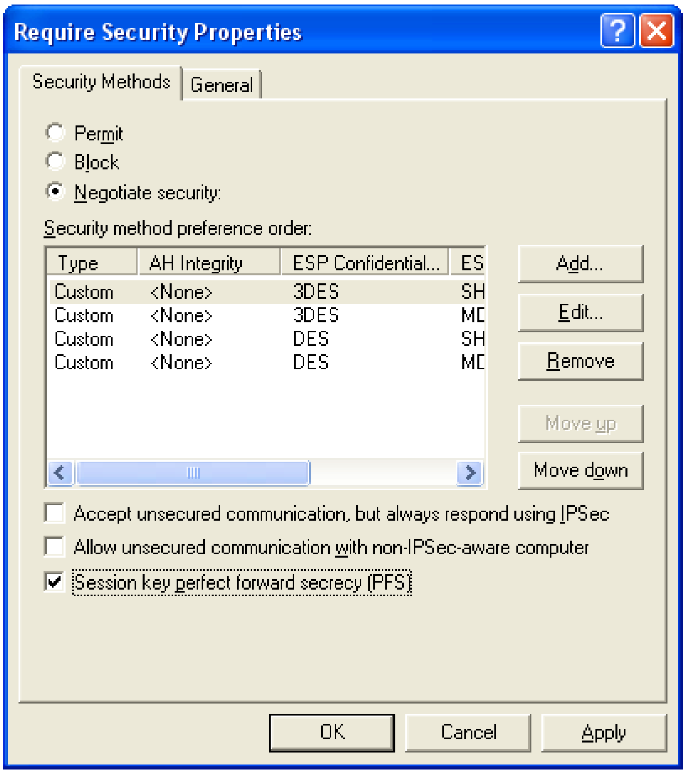


Figure 5.268 Require Security Properties

d. Verify that the 'Negotiate security' option is enabled, and deselect the 'Accept unsecured communication, but always respond using IPSec' check box. Select the 'Session key Perfect Forward Secrecy (PFS)' (the PFS option must be enabled on OpenRG), and click the OK button.

e. Under the 'Authentication Methods' tab, click the Edit button. The 'Edit Authentication Method Properties' window appears.

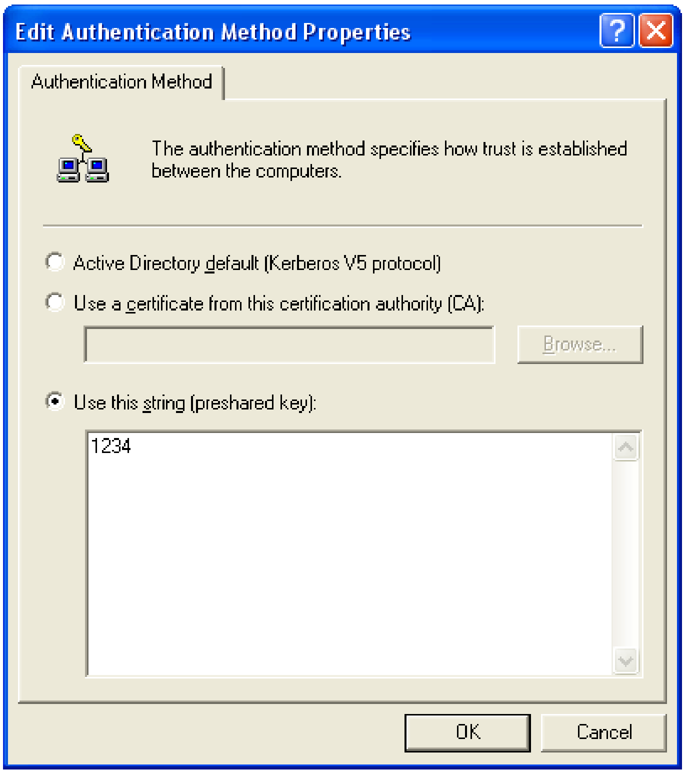


Figure 5.269 Edit Authentication Method Properties

f. Select the 'Use this string (preshared key)' radio button, and enter a string that will be used as the key (for example, 1234). Click the 'OK' button.

g. Under the 'Tunnel Setting' tab, select the 'The tunnel endpoint is specified by this IP Address' radio button, and enter <openrg_wan_ip>.

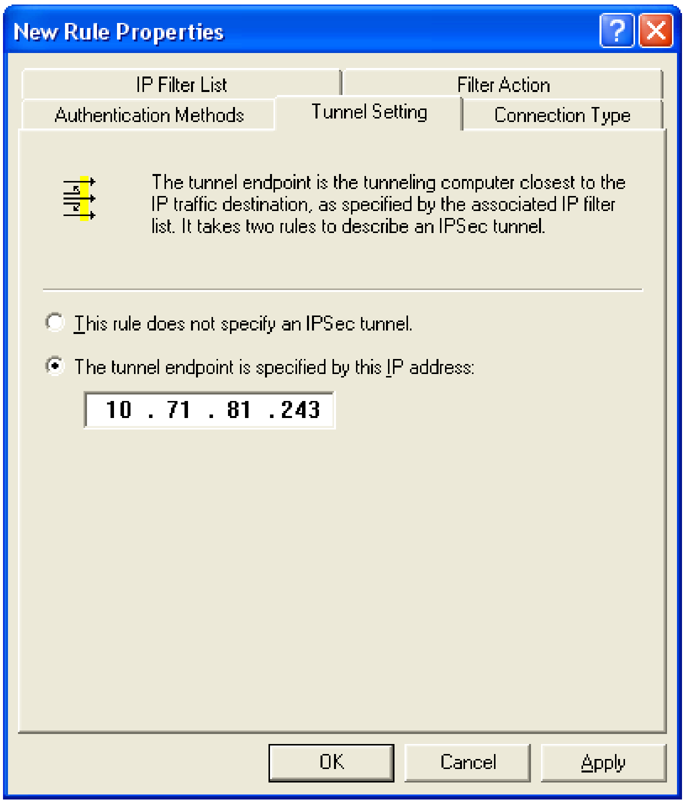


Figure 5.270 Tunnel Setting

h. Under the 'Connection Type' tab, verify that 'All network connections' is selected.

i. Click the 'Apply' button and then click the 'OK' button to save this rule.

5. Configuring Individual Rule of Tunnel 2 (OpenRG to Windows XP):

   a. Under the 'IP Filter List' tab of the 'New Rule Properties' window, select the 'OpenRG to Windows XP' radio button.

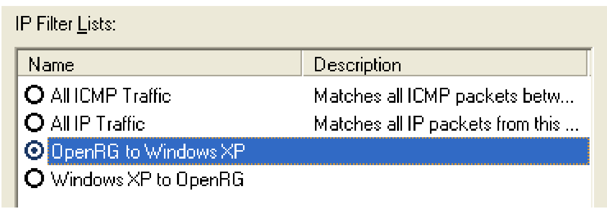


Figure 5.271 IP Filter List

   b. Click the 'Filter Action' tab (see Figure 5.267).

   c. Select the 'Require Security' radio button, and click the 'Edit' button. The 'Require Security Properties' window appears (see Figure 5.268).

   d. Verify that the 'Negotiate security' option is enabled, and deselect the 'Accept unsecured communication, but always respond using IPSec' check box. Select the

'Session key Perfect Forward Secrecy (PFS)' (the PFS option must be enabled on OpenRG), and click the OK button.

e. Under the 'Authentication Methods' tab, click the Edit button. The 'Edit Authentication Method Properties' window appears (see Figure 5.269).

f. Select the 'Use this string (preshared key)' radio button, and enter a string that will be used as the key (for example, 1234). Click the 'OK' button.

g. Under the 'Tunnel Setting' tab, select the 'The tunnel endpoint is specified by this IP Address' radio button, and enter <windows_ip>.

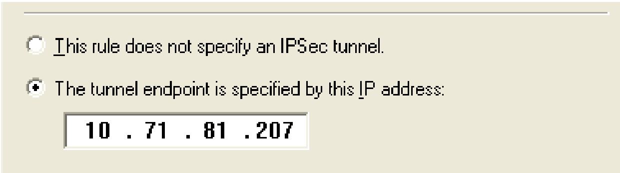


Figure 5.272 Tunnel Setting

h. Under the 'Connection Type' tab, verify that 'All network connections' is selected.

i. Click the 'Apply' button and then click the 'OK' button to save this rule.

j. Back on the 'OpenRG Connection Properties' window, note that the two new rules have been added to the 'IP Security rules' list.

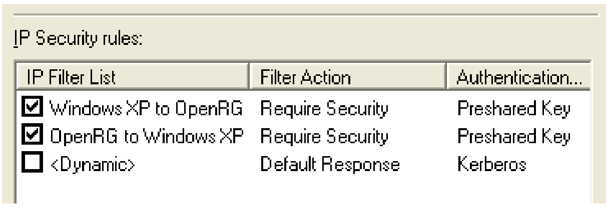


Figure 5.273 OpenRG Connection Properties

Click 'Close' to go back to the 'Local Security Settings' window (see Figure 5.256).

6. Assigning the New IPSec Policy: In the 'Local Security Settings' window, right-click the 'OpenRG Connection' policy, and select 'Assign'. A small green arrow will appear on the policy's folder icon and its status under the 'Policy Assigned' column will change to 'Yes'.

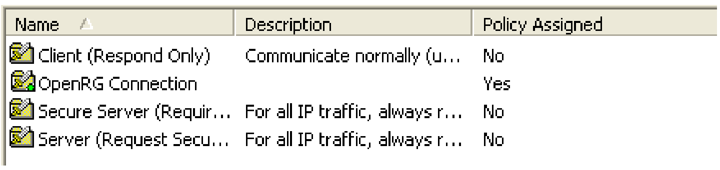


Figure 5.274 Local Security Settings

5.8.1.5 IPSec Gateway-to-Gateway Connection Scenario

Establishing an IPSec tunnel between Gateways A and B creates a transparent and secure network for clients from subnets A and B, who can communicate with each other as if they were inside the same network.

This section describes how to create a gateway to gateway IPSec tunnel with the following authentication methods:

- **Pre-shared Secret –** Developed by the VPN Consortium (VPNC). OpenRG's VPN feature is VPNC certified.
- **RSA Signature –** A method using an RSA signature that is based on OpenRG's public key.
- **Peer Authentication of Certificates –** A method using a Certificate Authority (CA).

This section describes the network configuration of both gateways, followed by the IPSec tunnel setup methods. The configurations of both gateways are identical, except for their IP addresses and the use of these addresses when creating the tunnel—the default gateway address of each gateway should be the WAN IP address of the other gateway.

> Note: This section describes the configuration of Gateway A only. The same configuration must be performed on Gateway B, with the exceptions that appear in the note admonitions.

The following figure describes the IPSec tunnel setup, and contains all the IP addresses involved. Use it as a reference when configuring your gateways.

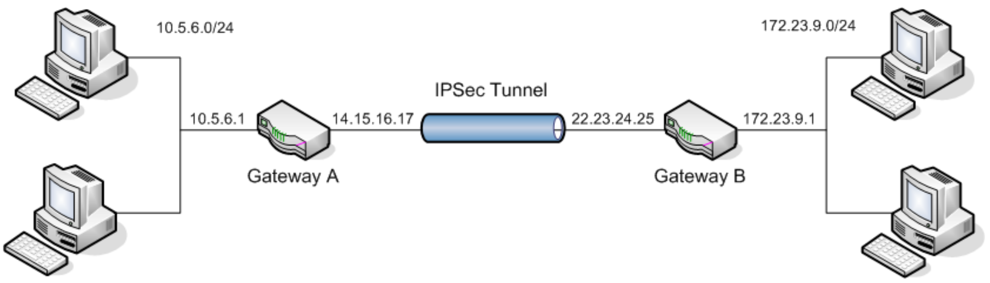


Figure 5.275 Configuration Diagram

5.8.1.5.1 Network Configuration

Before you can set up an IPSec connection, you must configure both of the gateways' LAN and WAN interface settings. This example contains specific IP addresses, which you can either use or substitute with your own.

- LAN Interface Settings

  1. Under the 'System' tab, click the 'Network Connections' menu item. The 'Network Connections' screen appears.

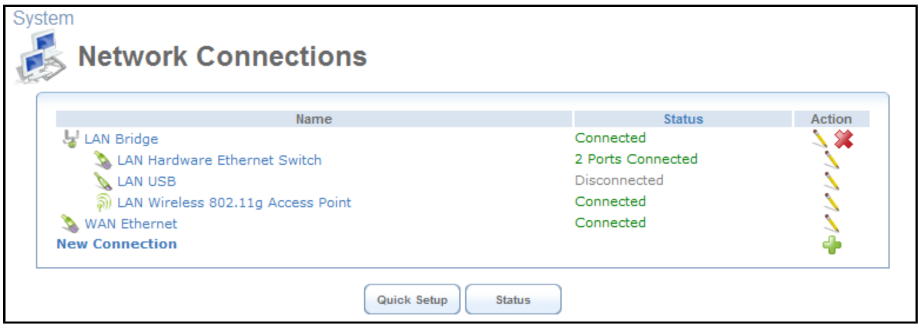


Figure 5.276 Network Connections

2. If your LAN Ethernet connection is bridged, click the 'LAN Bridge' link (as depicted in this example). Otherwise, click the 'LAN Ethernet' link (or the 'LAN Hardware Ethernet Switch' link, depending on your platform). The 'LAN Bridge Properties' screen appears.

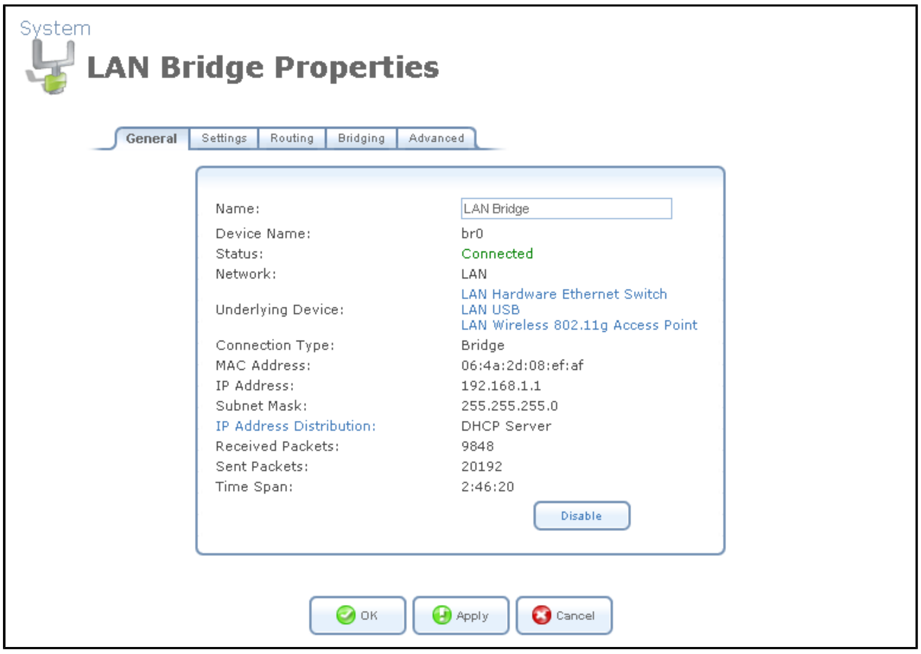


Figure 5.277 LAN Bridge Properties – General

3. Press the 'Settings' tab, and configure the following settings:

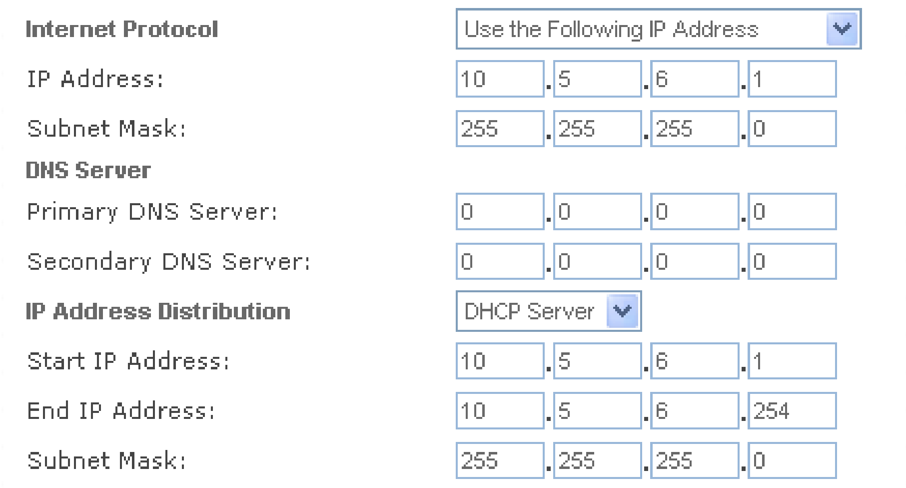


Figure 5.278 LAN Bridge Properties – Settings

Internet Protocol Select "Use the Following IP Address"

IP Address Specify 10.5.6.1

Subnet Mask Specify 255.255.255.0

IP Address Distribution Select "DHCP Server"

Start IP Address Specify 10.5.6.1

End IP Address Specify 10.5.6.254

Subnet Mask Specify 255.255.255.0

Note: When configuring Gateway B, the IP address should be 172.23.9.1, according to the example depicted here.

4. Click 'OK' to save the settings.

- WAN Interface Settings

1. Under the 'System' tab, click the 'Network Connections' menu item. The 'Network Connections' screen appears.

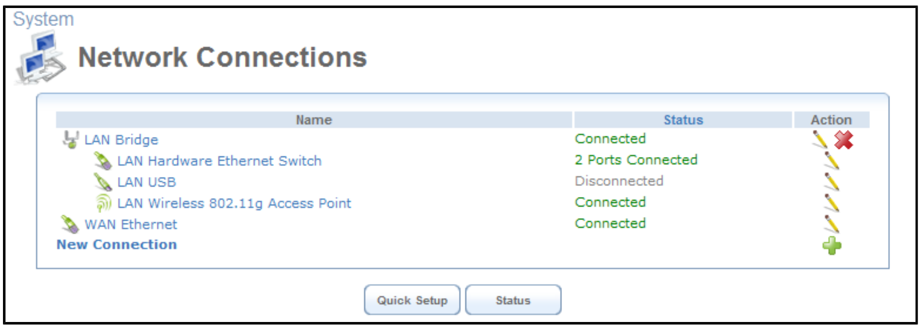


Figure 5.279 Network Connections

2. Click the 'WAN Ethernet' link, the 'WAN Ethernet Properties' screen appears.

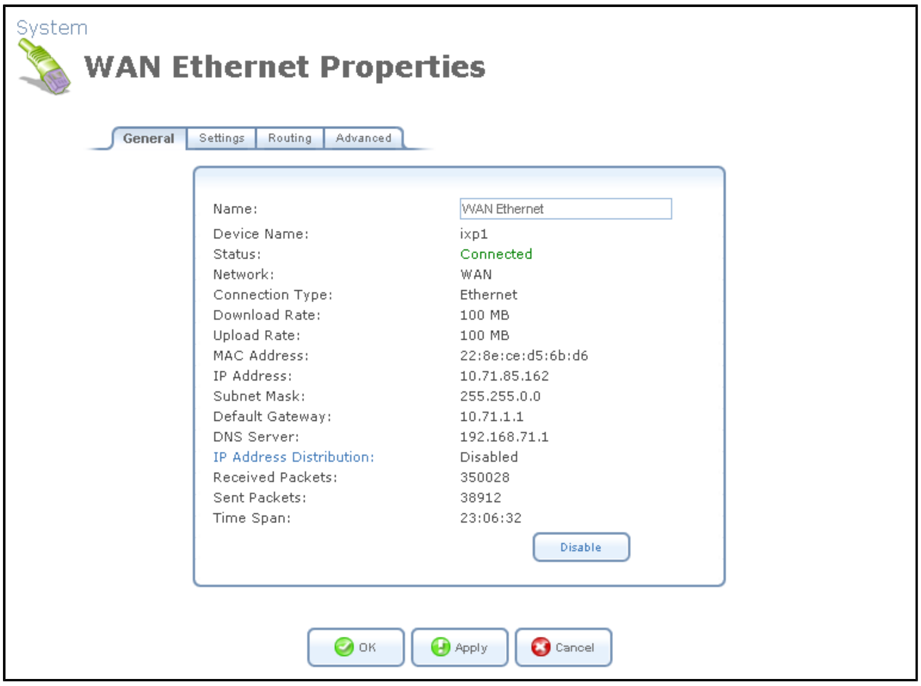


Figure 5.280 WAN Ethernet Properties – General

3. Press the 'Settings' tab, and configure the following settings:

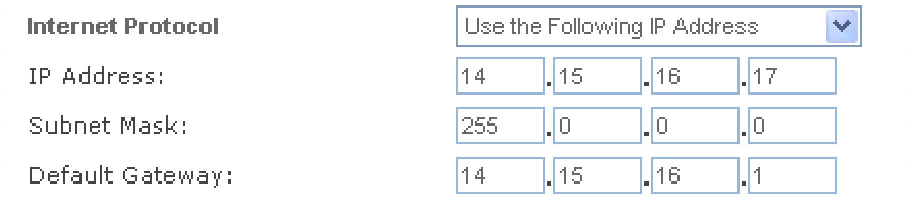


Figure 5.281 WAN Ethernet Properties – Settings

Internet Protocol Select "Use the Following IP Address"

IP Address Specify 14.15.16.17

Subnet Mask Specify the appropriate subnet mask, i.e 255.0.0.0

Default Gateway Specify the appropriate Default Gateway in order to enable IP routing, i.e 14.15.16.1

> Note: When configuring Gateway B, the IP address should be 22.23.24.25, and the default gateway 22.23.24.1, according to the example depicted here.

4. Click 'OK' to save the settings.

5.8.1.5.2 Gateway-to-Gateway with Pre-shared Secrets

A typical gateway-to-gateway VPN uses a pre-shared secret for authentication. Gateway A connects its internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17. Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. The Internet Key Exchange (IKE) Phase 1 parameters used are:

- Main mode
- 3DES (Triple DES)
- SHA-1
- MODP group 2 (1024 bits)
- Pre-shared secret of "hr5x"
- SA lifetime of 28800 seconds (eight hours) with no Kbytes re-keying

The IKE Phase 2 parameters used are:

- 3DES (Triple DES)
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for re-keying
- SA lifetime of 3600 seconds (one hour) with no Kbytes re-keying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

To set up Gateway A for this scenario, follow these steps:

1. Under the 'System' tab, click the 'Network Connections' menu item. The 'Network Connections' screen appears.

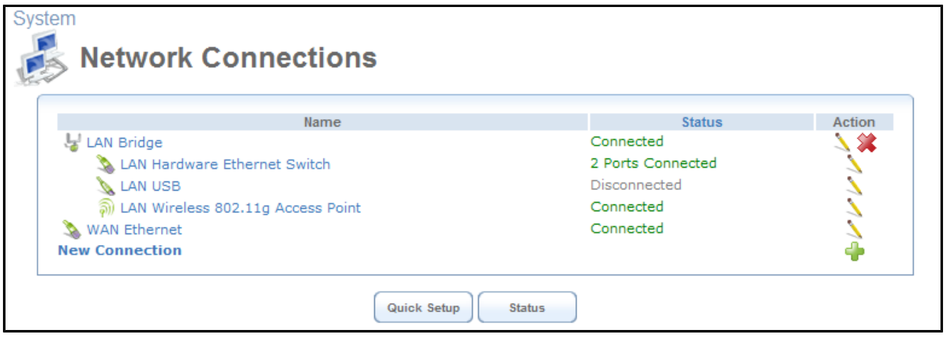


Figure 5.282 Network Connections

2. Click the 'New Connection' link. The 'Connection Wizard' screen appears.

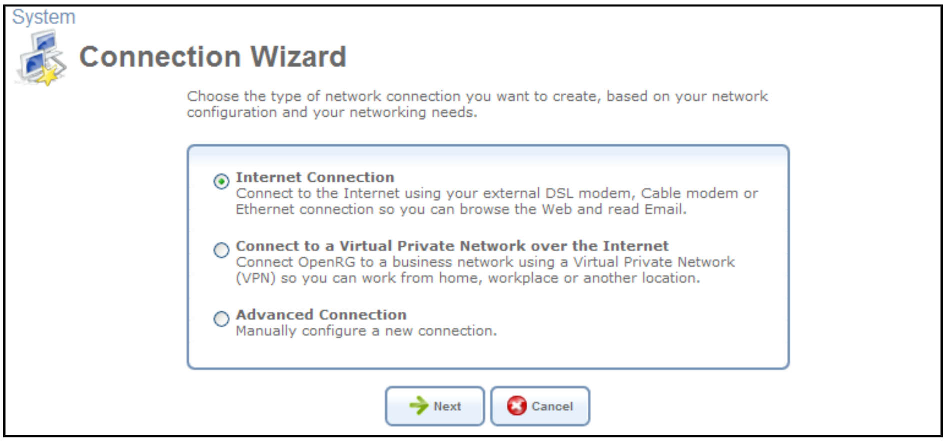


Figure 5.283 Connection Wizard

3. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears.

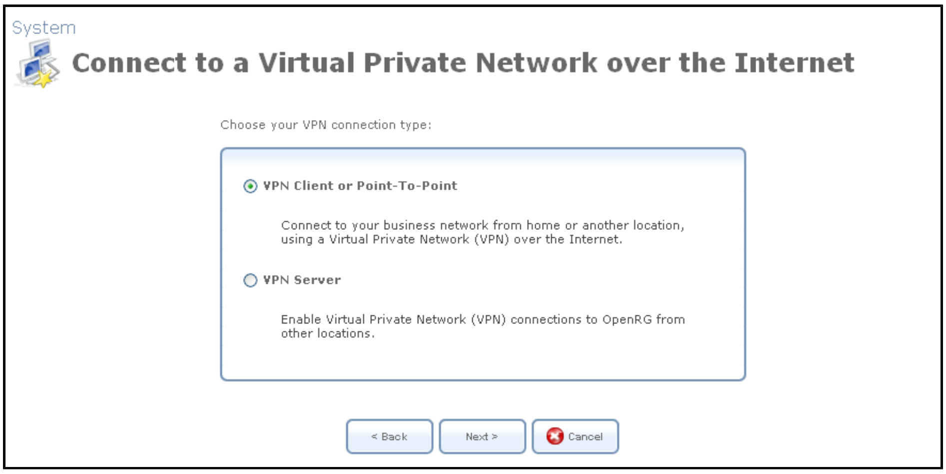


Figure 5.284 Connect to a Virtual Private Network over the Internet

4. Select the 'VPN Client or Point-To-Point' radio button and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

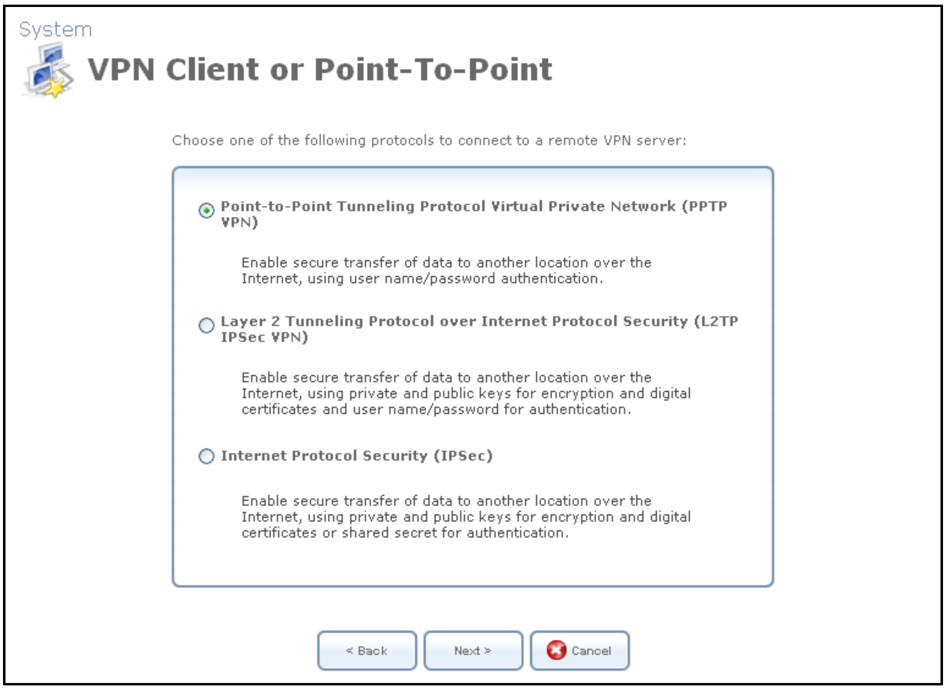


Figure 5.285 VPN Client or Point-To-Point

5. Select the 'Internet Protocol Security (IPSec)' radio button and click 'Next'. The 'Internet Protocol Security (IPSec)' screen appears.

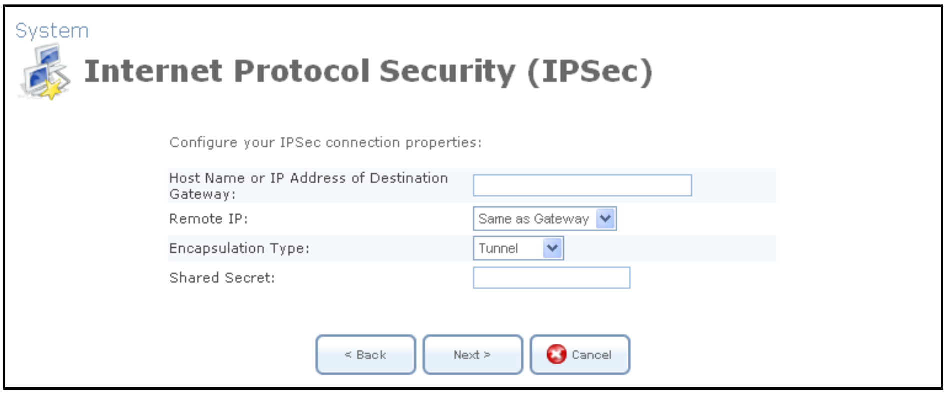


Figure 5.286 Internet Protocol Security (IPSec)

6. Specify the following parameters, as depicted in Figure 5.287.

Host Name or IP Address of Destination Gateway Specify 22.23.24.25

Remote IP Select "IP Subnet"

Remote Subnet IP Address Specify 172.23.9.0

Remote Subnet Mask Specify 255.255.255.0

Shared Secret Specify "hr5x"

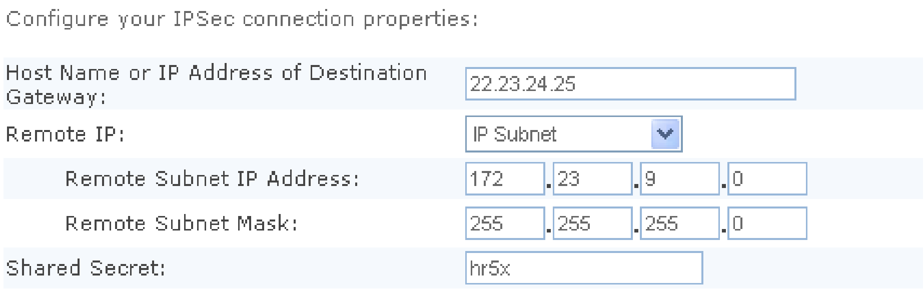


Figure 5.287 Internet Protocol Security (IPSec)

> Note: When configuring Gateway B, the IP Address of Destination Gateway should be 14.15.16.17, and the Remote Subnet IP Address should be 10.5.6.0, according to the example depicted here.

7. Click 'Next', the 'Connection Summary' screen appears.

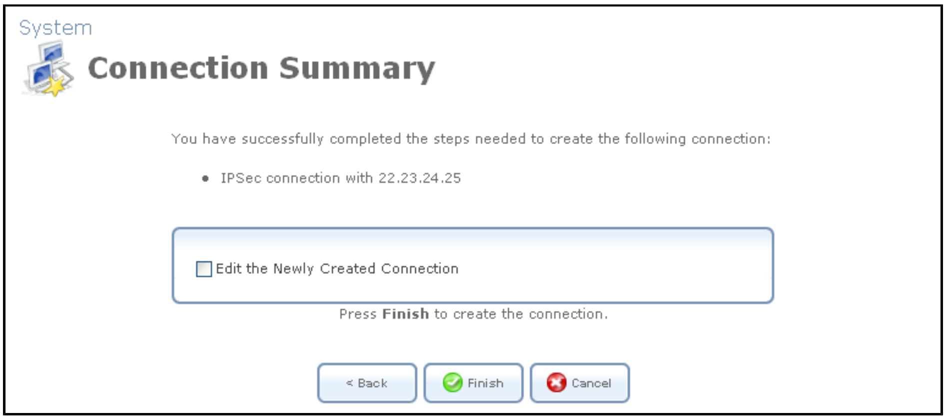


Figure 5.288 Connection Summary

8. Select the 'Edit the Newly Created Connection' check box, and click 'Finish'. The 'VPN IPSec Properties' screen appears, displaying the 'General' tab.

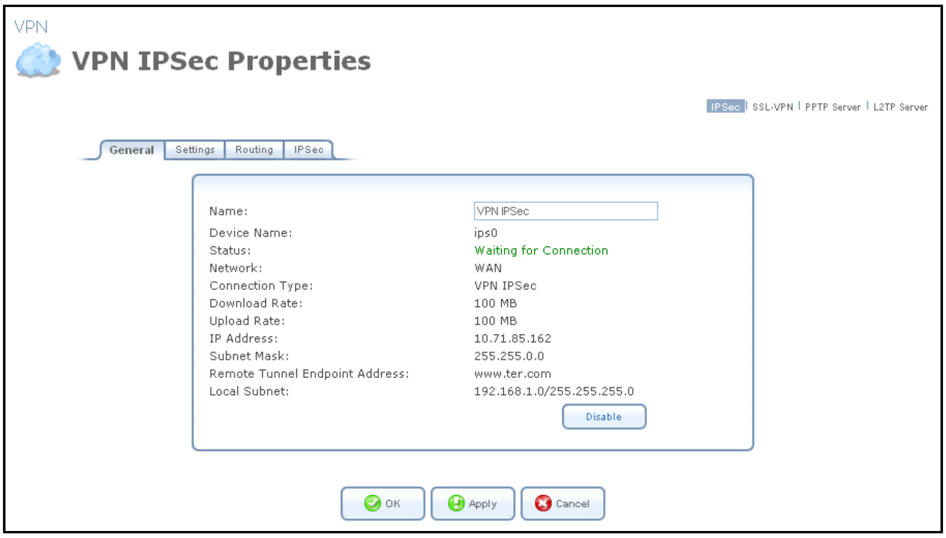


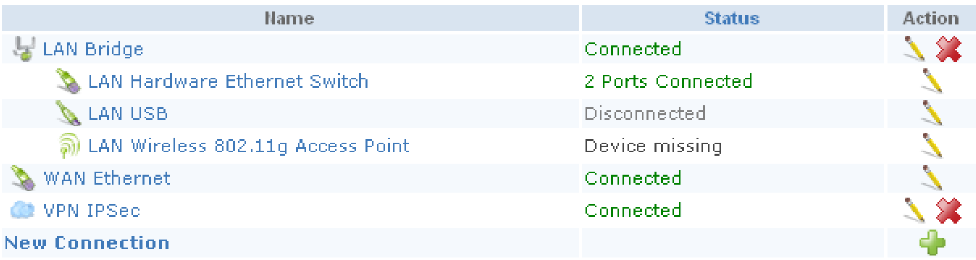
Figure 5.289 VPN IPSec Properties – General

9. Click the 'IPSec' tab, and configure the following settings:

   - Deselect the 'Compress' check box.
   - Under 'Hash Algorithm', deselect the 'Allow Peers to Use MD5' check box.
   - Under 'Group Description Attribute', deselect the 'DH Group 5 (1536 bit)' check box.
   - Under 'Encryption Algorithm', deselect the 'Allow AH Protocol (No Encryption)' check box.

10. Click 'OK' to save the settings.

Perform the same procedure on Gateway B with its respective parameters. When done, the IPSec connection's status should change to "Connected".



Name	Status	Action
LAN Bridge	Connected	
LAN Hardware Ethernet Switch	2 Ports Connected	
LAN USB	Disconnected	
LAN Wireless 802.11g Access Point	Device missing	
WAN Ethernet	Connected	
VPN IPSec	Connected	
New Connection		

Figure 5.290 Connected VPN IPSec Connection

5.8.1.5.3 Gateway-to-Gateway with an RSA Signature

The RSA signature, which is part of the RSA encryption mechanism, is an additional method available on OpenRG for providing peer authentication in a VPN IPSec connection. The RSA signature can be created in OpenRG on the basis of its public key. When using this method, the two gateways must be configured with each other's RSA signature, as further explained in this section.

To enable the gateway-to-gateway VPN IPSec connection using the RSA signature, perform the following:

1. Create a VPN IPSec connection on each gateway as described in Section 5.8.1.5.2.
2. In OpenRG **A**, go to the 'Advanced' screen, and click the 'IPSec' icon. The 'Internet Protocol Security (IPSec)' screen appears.

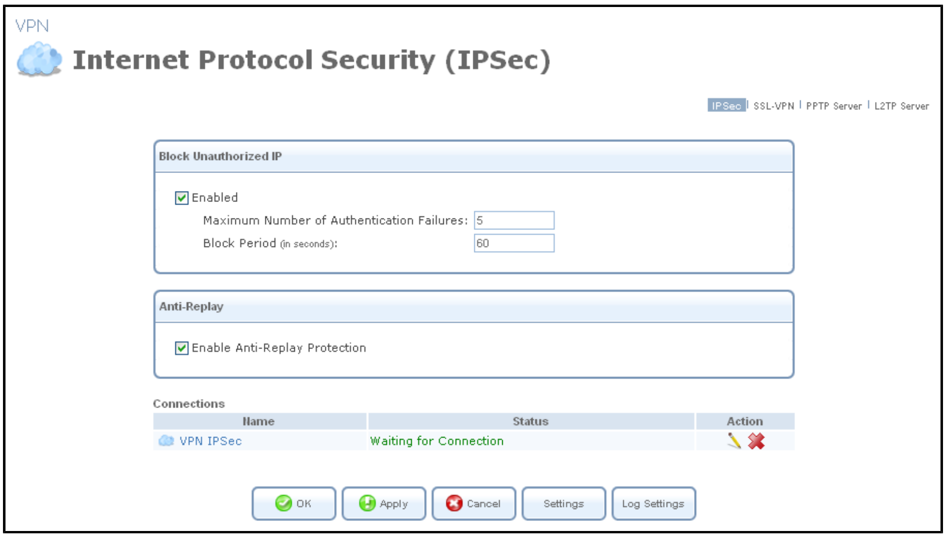


Figure 5.291 Internet Protocol Security (IPSec)

3. Click the 'Settings' button. The 'Internet Protocol Security (IPSec) Settings' screen appears, displaying OpenRG's public key.

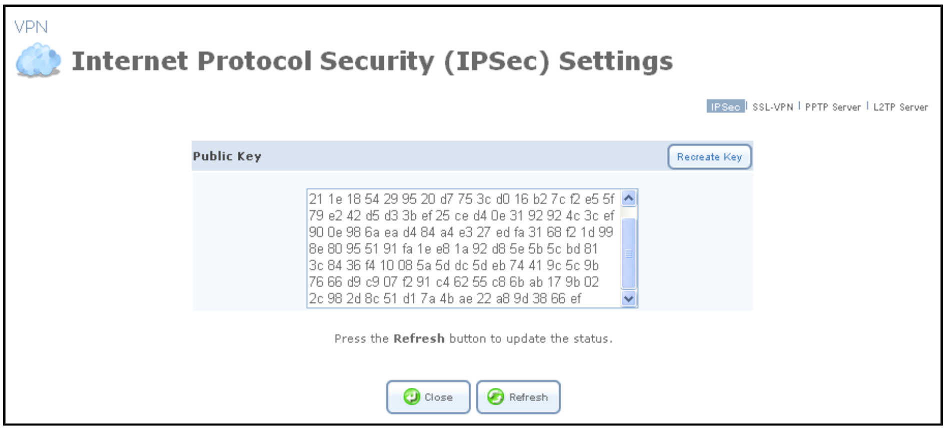


Figure 5.292 Internet Protocol Security (IPSec) Settings

4. Copy the public key and paste it into a text editor.

5. Remove all spaces from the public key so that it will appear as one string.

6. In OpenRG **B**, click the 'VPN' menu item under the 'Services' tab. The 'Internet Protocol Security (IPSec)' screen appears, displaying the VPN IPSec connection you have created (see Figure 5.291).

7. Click the connection's action icon , and select the 'IPSec' sub-tab of the 'VPN IPSec Properties' screen that appears (see Figure 5.289).

8. From the 'Peer Authentication' drop-down menu, select the 'RSA Signature' option. The screen refreshes, displaying the 'RSA Signature' text field.

9. In the text field, type **0x** and paste the public key string from the text editor.

10. Repeat the same procedure for configuring OpenRG **A** with the RSA signature of OpenRG **B**. When done, the IPSec connection's status on both gateways should change to 'Connected'.

5.8.1.5.4 Gateway-to-Gateway with Certificate-based Peer Authentication

An additional authentication method for a gateway-to-gateway VPN is peer authentication of certificates. Authentication is performed when each gateway presents a certificate, signed by a mutually agreed upon Certificate Authority (CA), to the other gateway.

For testing purposes, Linux provides a mechanism for creating self-signed certificates, thus eliminating the need to acquire them from the CA. This section provides a description for this procedure, after which you will be able to use these certificates for authentication of the gateway-to-gateway VPN connection.

To create a self-signed certificate, perform the following:

1. Running as root, install the OpenSSL Debian package:

   ```
   # apt-get install openssl
   ```

2. Switch back to a regular user, and create a directory for the certificates:

   ```
   $ cd ~
   $ mkdir cert_create
   $ cd cert_create/
   ```

3. Use the Linux 'CA.sh' utility. Note that only the required fields are listed below. For the rest, you may simply press Enter.

   ```
   $ /usr/lib/ssl/misc/CA.sh -newca
       Enter PEM pass phrase: <enter a password>
       Common Name: <enter your CA name>
       Enter pass phrase for ./demoCA/private/./cakey.pem: <enter a password>
   ```

   For more information about this script, run 'man CA.pl' (CA.pl and CA.sh are the same).

4. Copy the certificates from the **/demoCA** directory under which they were created, providing them with your CA name.

   ```
   $ cp demoCA/cacert.pem <your CA name>_cacert.pem
   $ cp demoCA/careq.pem <your CA name>_careq.pem
   ```

5. Load the new certificates to both gateways:

   a. Browse to the 'Advanced' tab and click the 'Certificates' icon.

   b. Select the 'CA's' sub-tab and click 'Upload Certificate'. The 'Load CA's Certificate' screen appears.

   c. Browse for the location of the certificate, which is **~/cert_create/<your CA name>_cacert.pem**, and click 'Upload'.

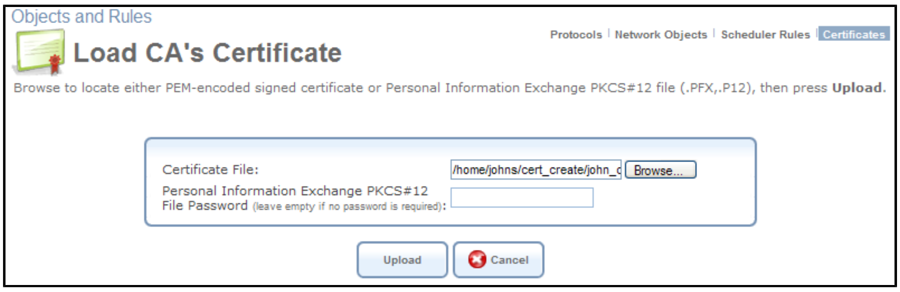


Figure 5.293 Load CA's Certificate

6. Generate a certificate request from both gateways:

   a. Browse to the 'Advanced' tab and click the 'Certificates' icon.

   b. In the 'OpenRG's Local' sub-tab, click 'Create Certificate Request'. The 'Create X509 Request' screen appears.

   c. In the 'Certificate Name' field, enter "OpenRG-1" (and "OpenRG-2" on the other gateway, respectively).

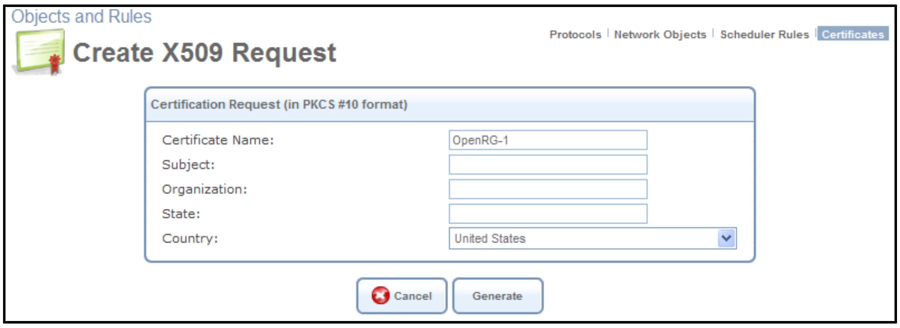


Figure 5.294 Create X509 Request

   d. Click 'Generate' and then 'Refresh'. The 'New X509 Request' screen appears.

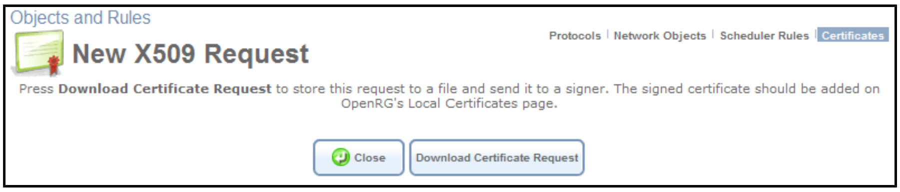


Figure 5.295 New X509 Request

   e. Click 'Download Certificate Request', and save the file under **~/cert_create/OpenRG-1/2_OpenRG.csr**.

> Note: Do not delete the empty certificate that now appears under the 'OpenRG's Local' sub-tab, as this is the request itself. If you delete it, the certificate will not be accepted by OpenRG.

7. Sign the certificate request using the 'CA.sh' script on both gateways:

```
$ mv <OpenRG-1>.csr newreq.pem
$ /usr/lib/ssl/misc/CA.sh -sign
    Enter pass phrase for ./demoCA/private/cakey.pem: <enter a password>
    Sign the certificate? [y/n]: <choose y>
    1 out of 1 certificate requests certified, commit? [y/n] <choose y>
$ mv newcert.pem <OpenRG-1>_newcert.pem
$ mv newreq.pem <OpenRG-1>_newreq.pem

<Repeat the above for OpenRG-2>
```

8. Load the certificates to both gateways:

   a. Browse to the 'Advanced' tab and click the 'Certificates' icon.

   b. In the 'OpenRG's Local' sub-tab, click 'Upload Certificate'. The 'Load OpenRG's Local Certificate' screen appears.

   c. Browse to the location of the certificate, which is **~/cert_create/<OpenRG-1/2>_newcert.pem**, and click 'Upload'.

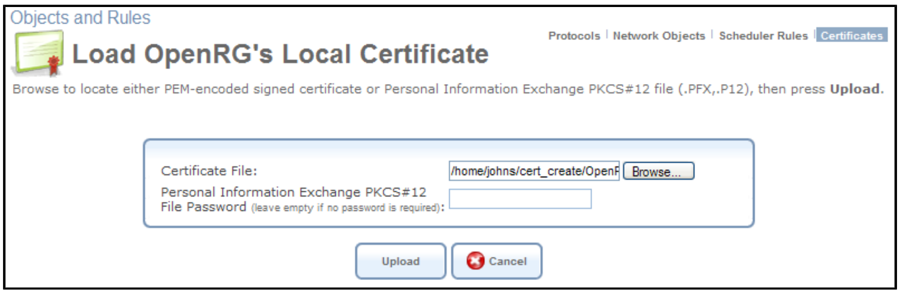


Figure 5.296 Load OpenRG's Local Certificate

To authenticate the VPN connection with the created certificates, perform the following:

1. Click the 'VPN IPSec' link in the 'Network Connections' screen, and then click the 'IPSec' sub-tab.

2. In the 'IPSec Automatic Phase 1' section, in the 'Peer Authentication' drop-down menu, select "Certificate". The screen refreshes, providing additional settings.

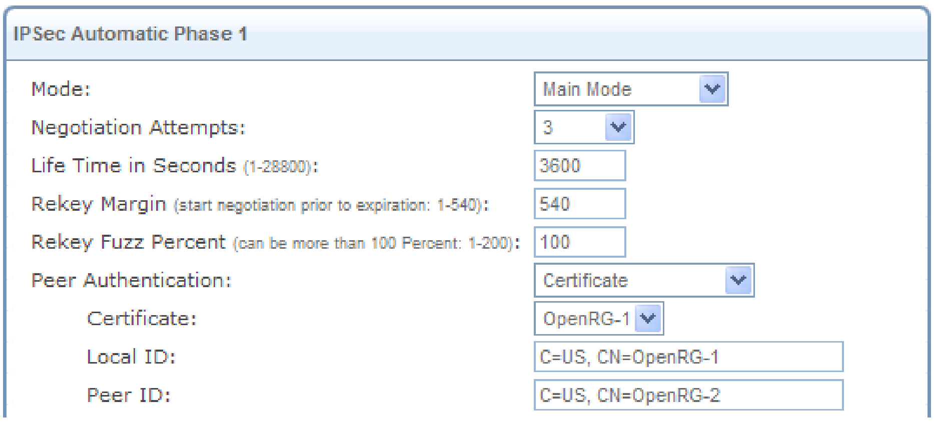


Figure 5.297 VPN IPSec Properties

3. In the 'Certificate' drop-down menu, select Gateway A's newly added certificate.

4. In the 'Local ID' field, enter Gateway A's certificate details. You can copy these details from the 'Certificates' screen under the 'Advanced' tab. Click the certificate and copy the details from the subject field, for example "C=US, CN=OpenRG-1".

5. In the 'Peer ID' field, enter Gateway B's certificate details, for example "C=US, CN=OpenRG-2".

6. Click 'OK' to save the settings.

Perform the same procedure on Gateway B with its respective parameters. When done, the IPSec connection's status should change to "Connected".

Name	Status	Action
LAN Bridge	Connected	
LAN Hardware Ethernet Switch	2 Ports Connected	
LAN USB	Disconnected	
LAN Wireless 802.11g Access Point	Device missing	
WAN Ethernet	Connected	
VPN IPSec	Connected	
New Connection		

Figure 5.298 Connected VPN IPSec Connection

5.8.2 Secure Socket Layer VPN

Secure Socket Layer Virtual Private Network (SSL VPN) provides simple and secure remote access to home and office network resources. It provides the security level of IPSec, but with the simplicity of using a standard Web browser. The unparalleled advantage of SSL VPN is its zero-configuration on the client's end. Remote users can simply browse to OpenRG from any computer in the world and run applications on its LAN computers. However, since SSL VPN is not a tunnel such as PPTP or IPSec, only pre-defined applications may be used. When using this feature, non-administrator remote users browsing to OpenRG will be routed to the "SSL VPN Portal". This portal will present them each with their list of applications.

> Note: The only requirement for the client computer is the availability of Java Runtime Environment (JRE), which is mandatory for using this feature. Use the "Click here" link at the bottom of the SSL VPN portal screen to install this environment, or visit http://www.sun.com.

5.8.2.1 Using SSL VPN – the Remote Desktop Example

This section demonstrates setting up a Remote Desktop (RDP) application over SSL VPN in order to remotely connect and control a computer inside OpenRG's LAN. This consists of two stages—creating a remote desktop global shortcut, and launching the application from a remote computer via the SSL VPN portal.

5.8.2.1.1 Creating a Global Shortcut

To create an RDP shortcut, perform the following:

1. Access the Secure Socket Layer VPN (SSL VPN) settings either from its link under the 'VPN' menu item of the 'Services' screen, or by clicking the 'SSL VPN' icon in the 'Advanced' screen. The 'SSL VPN' screen appears.

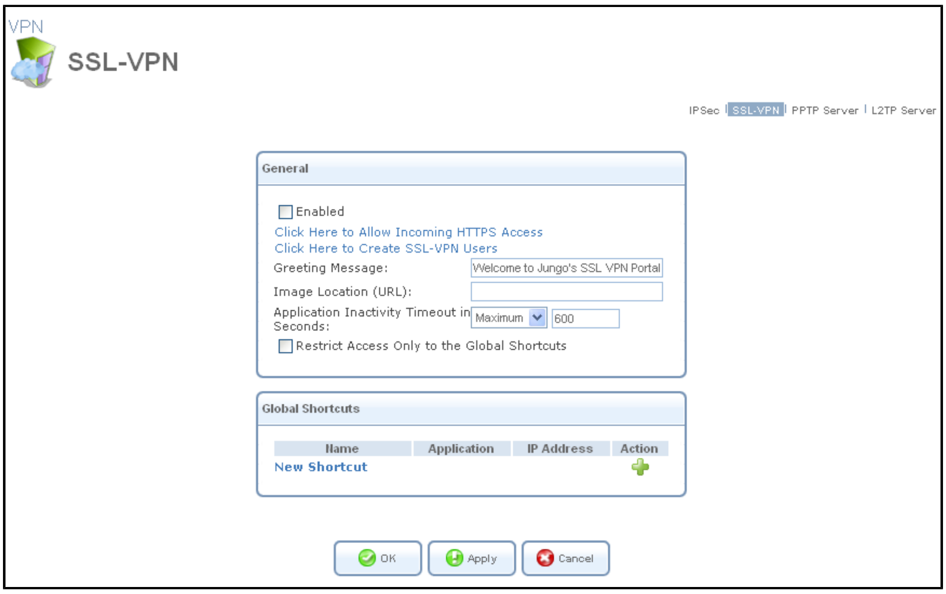


Figure 5.299 SSL VPN

2. To enable SSL VPN, select the 'Enabled' check box, and click 'Apply'. The screen refreshes, adding a link to the SSL VPN Portal.

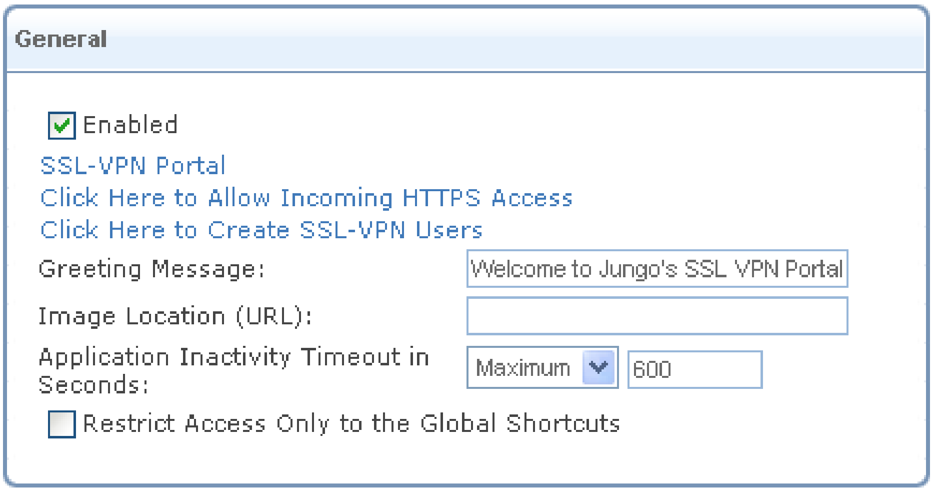


Figure 5.300 Enabled SSL VPN

This link opens the SSL-VPN portal that remote users will access when browsing to OpenRG, as described in Section 5.8.2.3.

3. Click the 'Click Here to Allow Incoming HTTPS Access' link. The 'Remote Administration' screen appears (for more information, refer to Section 6.7.3). In the 'Allow Incoming WAN Access to Web-Management' section, select both HTTPS port 443 and 8443, and click 'OK'.

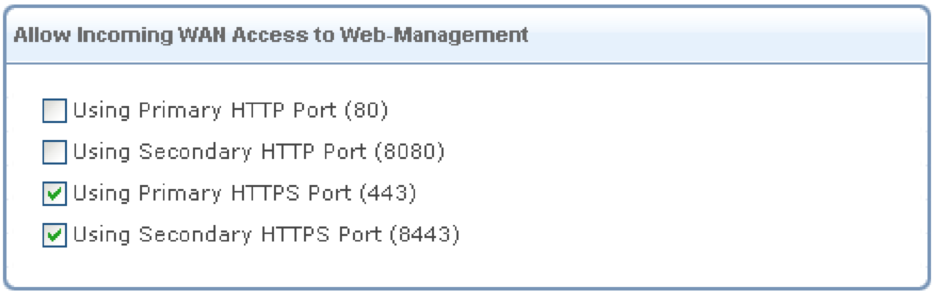


Figure 5.301 Remote Administration Ports

4. Back in the 'SSL VPN' screen, click the 'Click Here to Create SSL-VPN Users' link. The 'Users' screen appears, where you can define a user with the 'Remote Access by SSL VPN' option enabled. Refer to Section 6.3 to learn how to define and configure users. You can specify a group of users in the same manner.

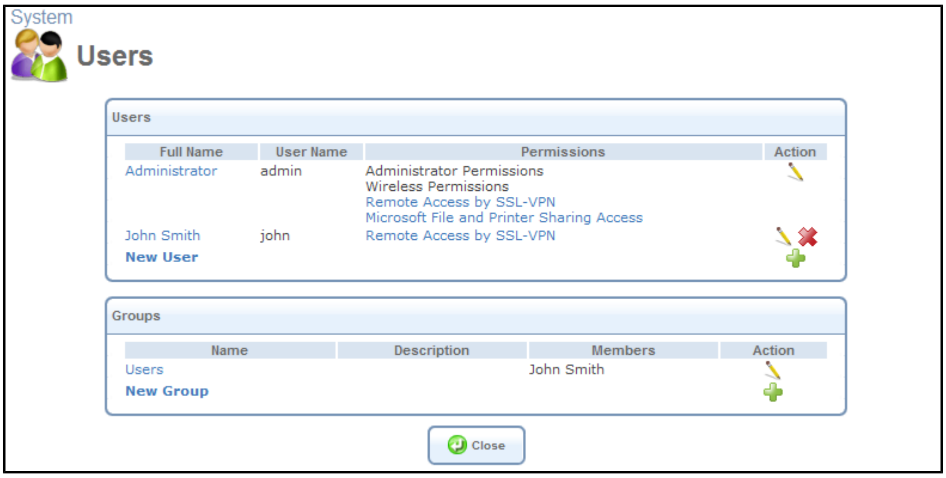


Figure 5.302 New User

Click 'Close' when done.

5. In the 'SSL VPN' screen, click the 'New Shortcut' link. The 'Shortcut Wizard' screen appears.

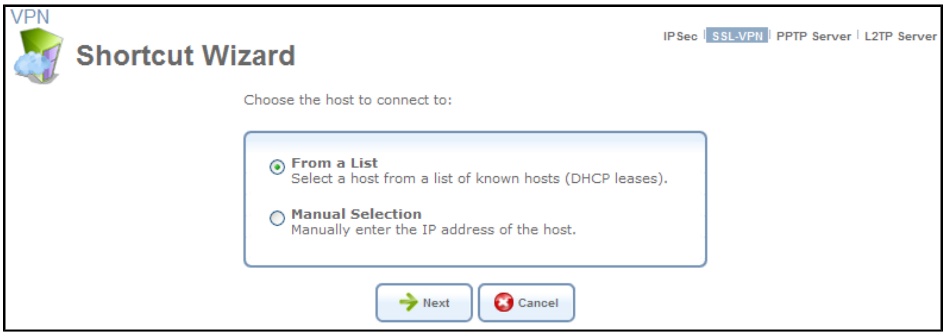


Figure 5.303 New Shortcut

6. Choose whether to select a host from a given list, comprised of DHCP leases that are known to OpenRG, or to manually enter the host's IP address, and click 'Next'. If you

choose 'From a List', the following screen appears. Select the host to which you would like to add a shortcut, and click 'Next'.

Figure 5.304 Choose Host from List

The next wizard screen appears, either with the IP address of a selected host, or without an IP address for manual selection.

Figure 5.305 Select and Configure an Application

7. In the 'Application' drop-down menu, select 'Remote Desktop (RDP)'. The screen refreshes, displaying the RDP parameters.

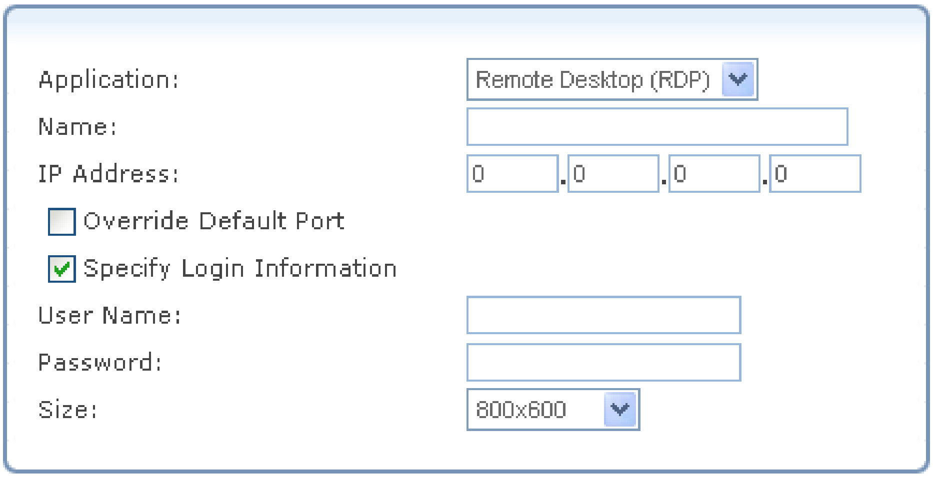


Figure 5.306 RDP Parameters

8. In this screen, perform the following:

a. Enter a name for the shortcut.

b. Enter the IP address of the LAN computer on which the RDP will be performed.

c. Select the 'Override Default Port' option if the LAN computer uses a port other than the application's "well known" default port. An additional field appears, in which you must enter the alternative port.

d. If you choose the default setting of requiring the user to specify login information when connecting with RDP, provide the username and password that are used to login to the LAN computer.

e. Select the size of the screen in which the remote desktop application will be displayed.

Click 'Next'. The 'Shortcut Summary' screen appears.

Figure 5.307 Shortcut Summary

9. Select the 'Edit the Newly Created Shortcut' check box in order to associate a user or a group with this shortcut, and click 'Finish'. The 'Edit Shortcut' screen appears.

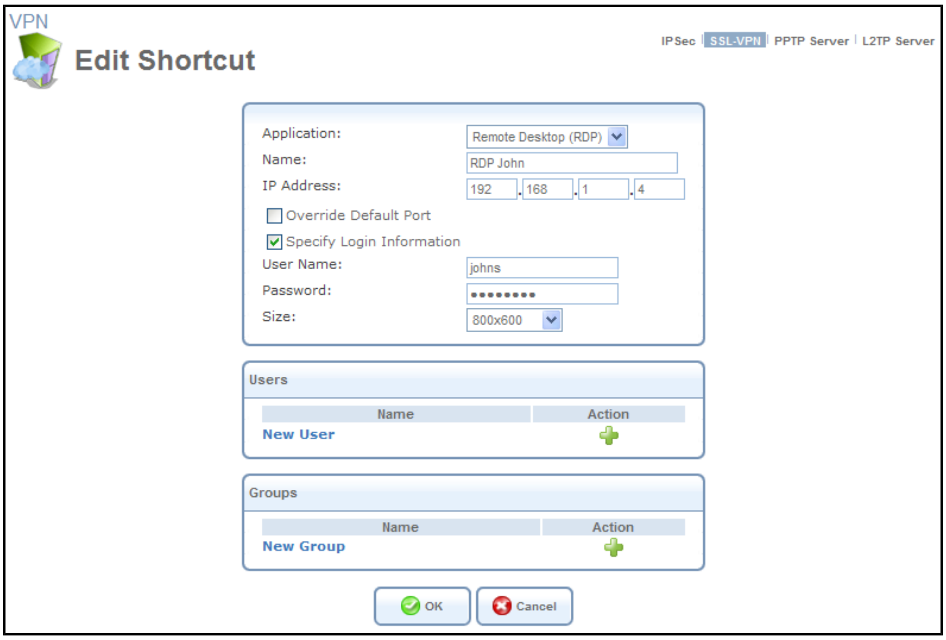


Figure 5.308 Edit Shortcut

10. Click the 'New User' link (or 'New Group' according to your preference), and select a user with remote SSL VPN access permission from the drop-down menu.

Figure 5.309 User

11. Click 'OK'. The new user is added to the 'Users' section in the 'Edit Shortcut' screen.

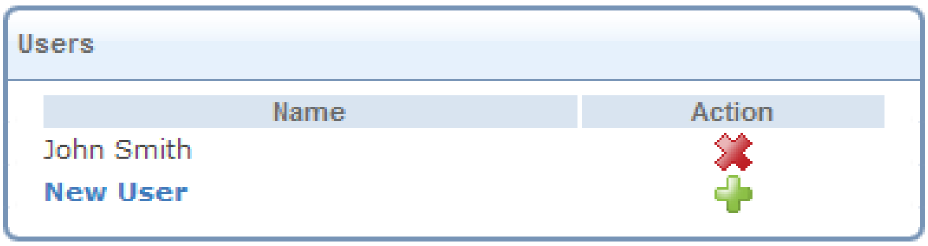


Figure 5.310 Associated User

12. Click 'OK' to save the settings. The new shortcut is added to the 'Shortcuts' screen, and will be available for this user when connecting to the SSL VPN portal.

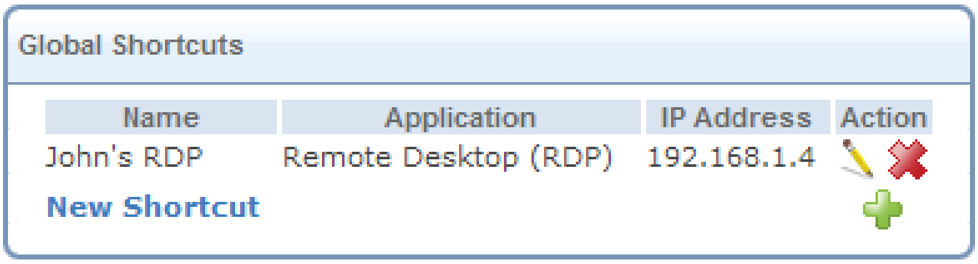


Figure 5.311 Global Shortcuts

5.8.2.1.2 Launching the Application

To launch the remote desktop application from a remote computer, perform the following:

1. Browse to OpenRG from a remote computer by typing **https://<OpenRG's Internet address>** (OpenRG's Internet address can be found under the 'Internet Connection' tab). For example, **https://10.71.86.21**.

2. Log in with the newly added user. The portal screen appears.

Figure 5.312 SSL VPN Portal

3. Click the 'Shortcuts' button. The 'Shortcuts' screen appears, displaying shortcuts to the available applications.

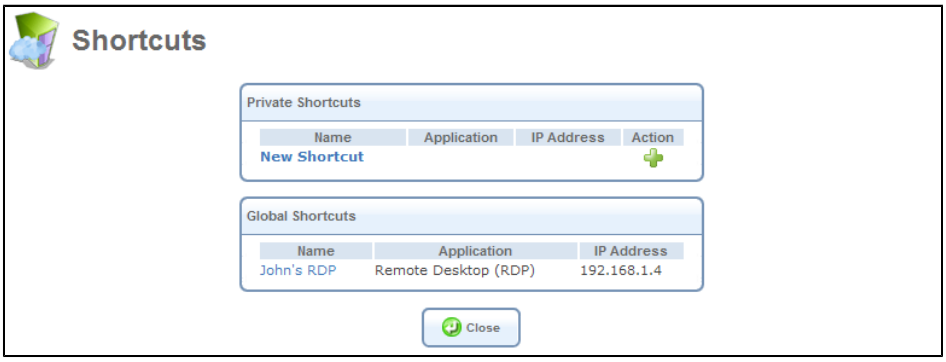


Figure 5.313 Shortcuts

4. Click the name of the RDP shortcut. A Remote Desktop session screen opens, prompting you for login details. Enter the computer's login username and password to gain RDP

control. If an RDP screen fails to load, check that JRE is properly installed on the client computer.

5.8.2.2 Using Other Applications over SSL VPN

OpenRG provides the following popular applications that remote users can use to access the home network in order to perform various tasks. To set up an application, follow the remote desktop example described in the previous section. The only difference between the setups of the applications is in the parameters defined in the 'Shortcut Wizard' screen, as described in the following sections.

5.8.2.2.1 Web-based CIFS

This option enables the remote user to share files with a computer inside OpenRG's LAN using Jungo's Web-based Common Internet File System (Web-based CIFS). File sharing is performed from within the WBM, which displays the LAN computer's file system, and enables a vast set of actions described later in this section. In addition, this method does not require installing JRE, since no third-party software is used. In the 'Shortcut Wizard' screen, configure the following parameters.

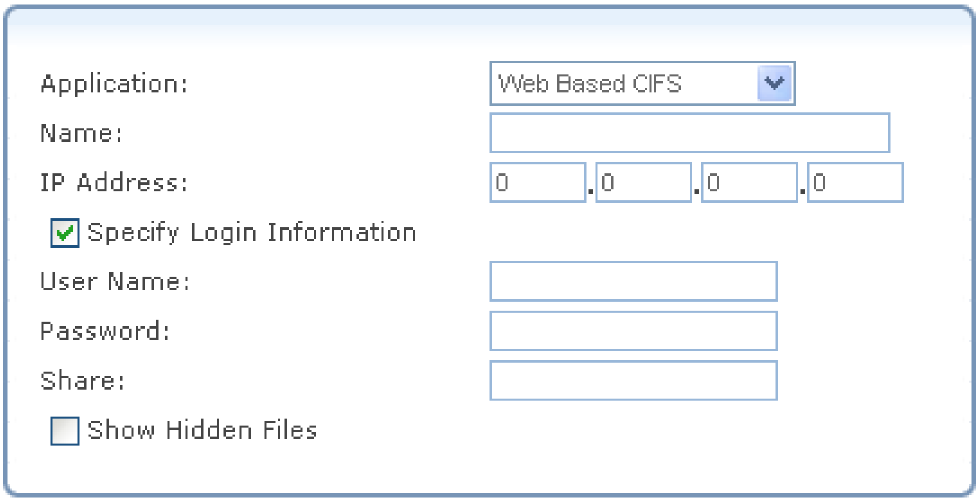


Figure 5.314 Web-based CIFS Parameters

Name Enter a name for this shortcut.

IP Address Enter the IP address of the LAN computer on which to perform the application.

Specify Login Information If the LAN computer requires a login, specify the following parameters to auto-login when launching the application:

User Name The user name with which to login.

Password The password with which to login.

Share Specify the name of the share directory on which to perform the application.

Show Hidden Files Select this check box to allow showing of hidden files.

Once you configure a shortcut to Web-based CIFS and associate it with a user (or group), you can use the application when logged into the SSL VPN portal as that user, by clicking the shortcut link that appears in the 'Shortcuts' screen.

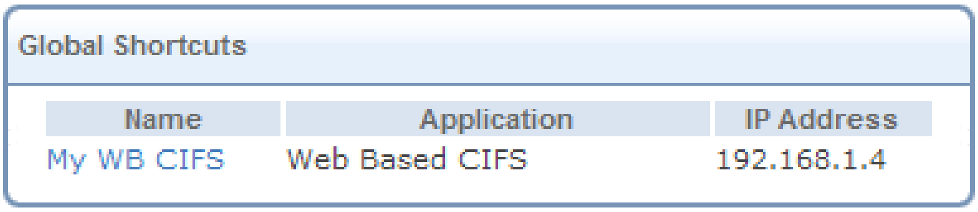


Figure 5.315 Shortcut to Web-based CIFS

If you had not specified a share directory name when configuring the shortcut, the link will lead you to the base directory of the host with the specified IP address.

Figure 5.316 Web-based CIFS Host

If you had specified a share directory name when configuring the shortcut (in this example —"home"), the link will lead you to the share directory on the specified host.

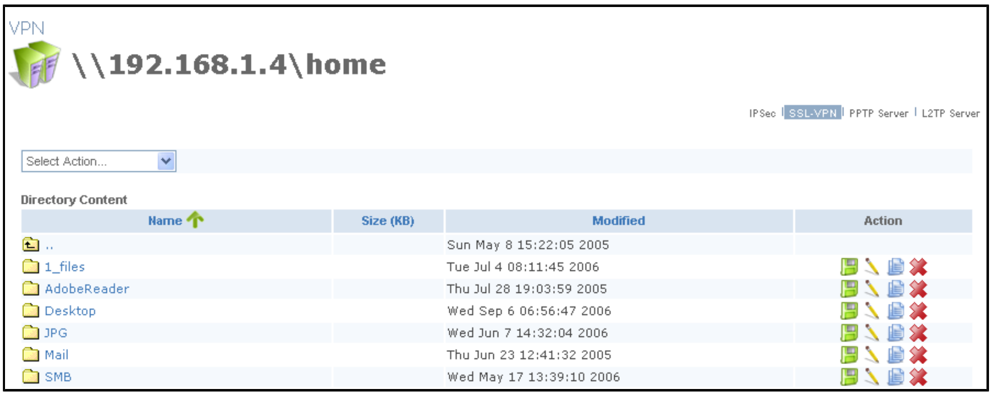


Figure 5.317 Web-based CIFS Share

The directory content is displayed, with the file name, size, last modification and actions you may perform on the file. You can browse the directory contents and sort the columns according to the file name, size or modification date. The action icons for each file and directory allow you to perform the following:

- Download

> Note: Directories are downloaded as tarball archives (in ***.tar** format).

- Rename

- Copy to Clipboard
- Remove

You can perform additional actions using the drop-down menu.

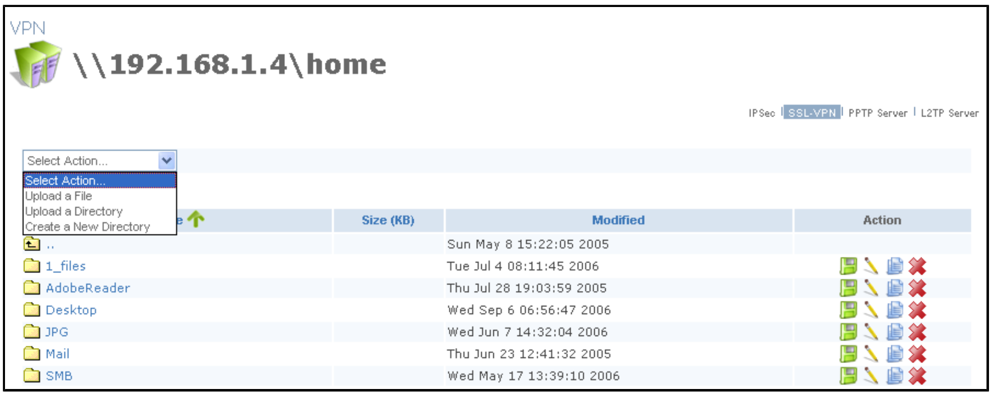


Figure 5.318 Web-based CIFS Actions

- **Upload a File** Select this option to upload a file to the share. The screen refreshes.

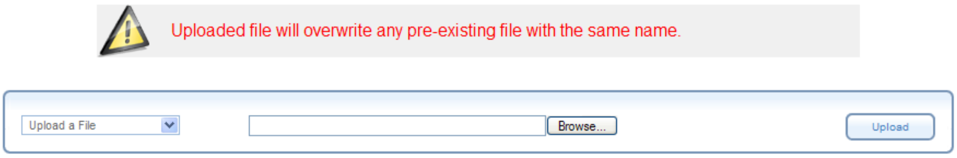


Figure 5.319 Upload a File

Enter the location of the file to upload, or click the 'Browse' button to browse for the file. Click the 'Upload' button to upload the file.

- **Upload a Directory** You can also upload an entire directory of files, by performing the following:

  1. Create a tarball archive out of the target directory.
  2. Enter the location of the archive, or click the 'Browse' button to browse to its location.
  3. Click the 'Upload' button to upload the archive.

- **Create a new Directory** You can create a new directory by simply typing its name and clicking the 'Go' button.

- **Paste from Clipboard** This option appears only after using the 'Copy to Clipboard' option ( action icon) to copy a directory or file from one directory to another.

5.8.2.2.2 CIFS

This option enables the remote user to share files with a computer inside OpenRG's LAN using the Common Internet File System (CIFS). The protocol allows to manipulate files on a network

computer just as if they were on the remote computer. Operations such as read, write, create, delete, and rename are all supported. In the 'Shortcut Wizard' screen, configure the following parameters.

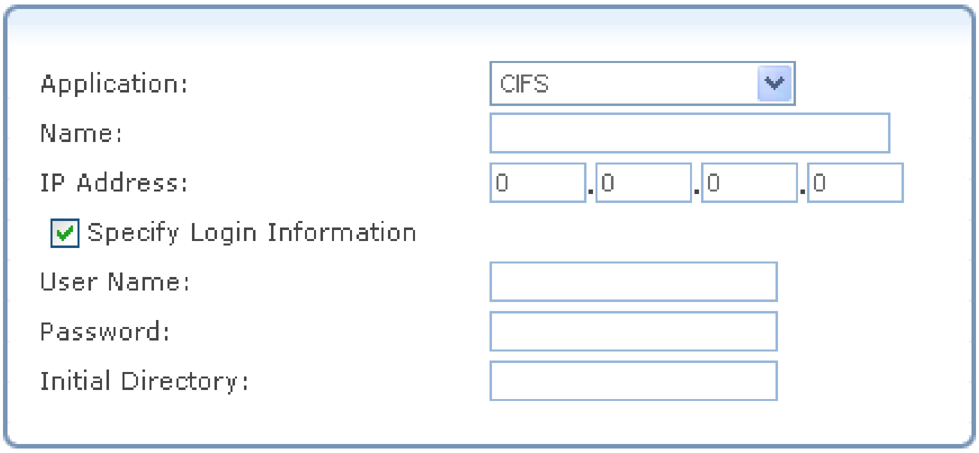


Figure 5.320 CIFS Parameters

Name Enter a name for this shortcut.

IP Address Enter the IP address of the LAN computer on which to perform the application.

Specify Login Information If the LAN computer requires a login, specify the following parameters to auto-login when launching the application:

User Name The user name with which to login.

Password The password with which to login.

Initial Directory Specify the root directory on which to perform the application. For example, **A/**, **C:\Program Files**, etc.

Once you configure a shortcut to CIFS and associate it with a user (or group), you can use the application when logged into the SSL VPN portal as that user, by clicking the shortcut link that appears in the 'Shortcuts' screen.

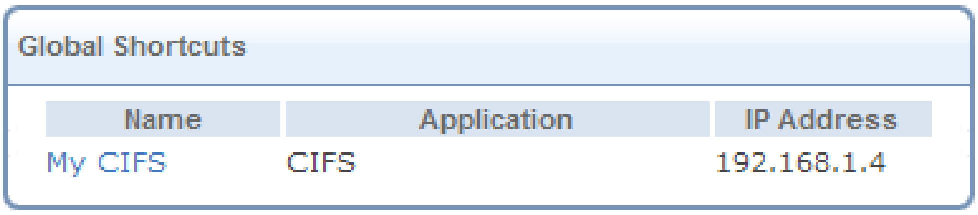


Figure 5.321 Shortcut to CIFS

5.8.2.2.3 VNC

This option enables the remote user to connect and control a computer inside OpenRG's LAN using the Virtual Network Connection (VNC) application (similar to RDP). In the 'Shortcut Wizard' screen, configure the following parameters.

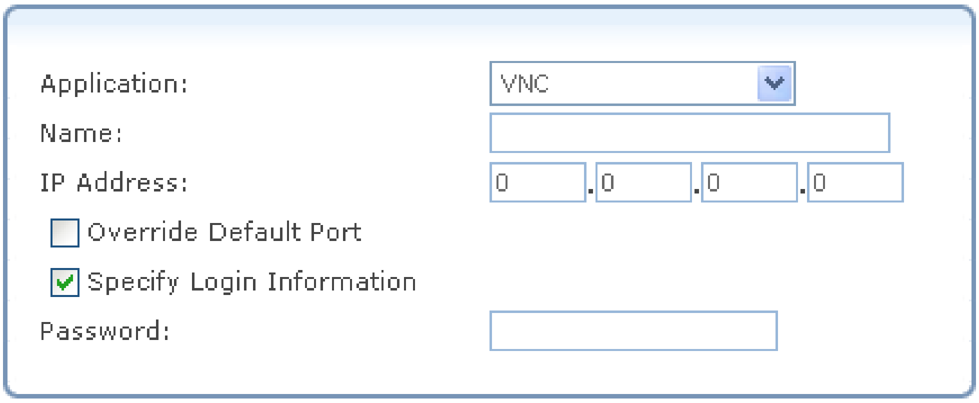


Figure 5.322 VNC Parameters

Name Enter a name for this shortcut.

IP Address Enter the IP address of the LAN computer on which to perform the application.

Override Default Port Select this option if the LAN computer uses a port other than the application's "well known" default port. An additional field appears, in which you must enter the alternative port.

Specify Login Information If the LAN computer requires a login, specify the following parameter to auto-login when launching the application:

Password The password with which to login.

Once you configure a shortcut to VNC and associate it with a user (or group), you can use the application when logged into the SSL VPN portal as that user, by clicking the shortcut link that appears in the 'Shortcuts' screen.

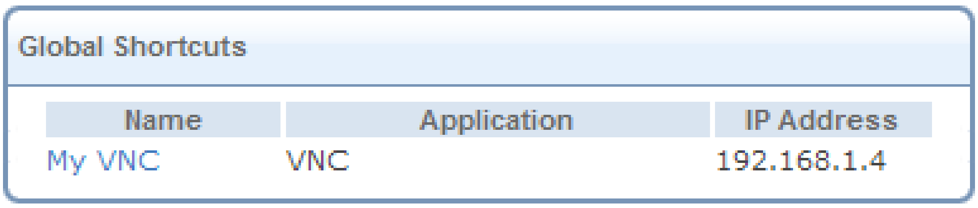


Figure 5.323 Shortcut to VNC

5.8.2.2.4 FTP

This option enables the remote user to transfer files between the remote computer and a computer inside OpenRG's LAN using the File Transfer Protocol (FTP) application. Note that an FTP server must be installed on the LAN computer. In the 'Shortcut Wizard' screen, configure the following parameters.

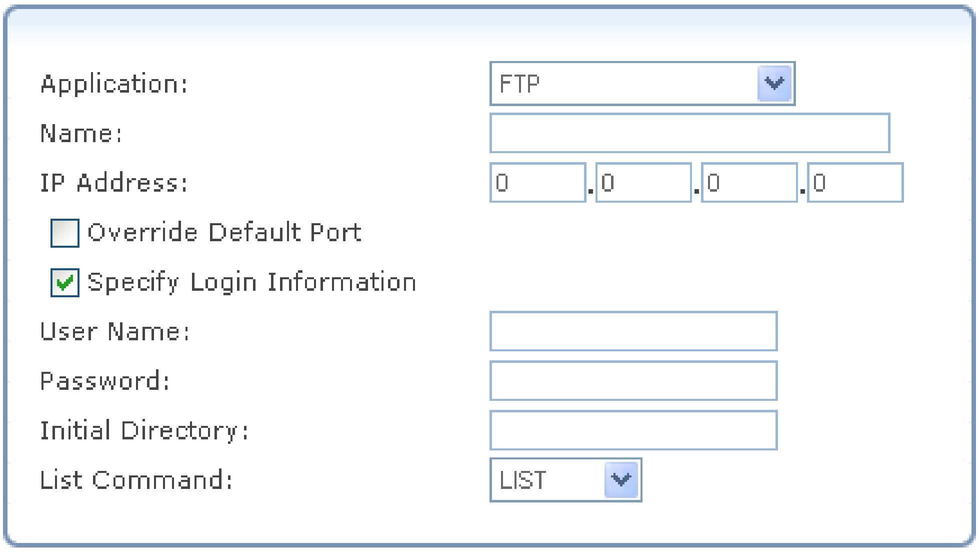


Figure 5.324 FTP Parameters

Name Enter a name for this shortcut.

IP Address Enter the IP address of the LAN computer on which to perform the application.

Override Default Port Select this option if the LAN computer uses a port other than the application's "well known" default port. An additional field appears, in which you must enter the alternative port.

Specify Login Information If the LAN computer requires a login, specify the following parameters to auto-login when launching the application:

User Name The user name with which to login.

Password The password with which to login.

Initial Directory Specify the root directory on which to perform the application. For example, **A/**, **C:\Program Files**, etc.

List Command Select the FTP command that determines the list of files and their properties available for FTP. You should only change this option if the LAN computer does not support the default "LIST" command.

Once you configure a shortcut to FTP and associate it with a user (or group), you can use the application when logged into the SSL VPN portal as that user, by clicking the shortcut link that appears in the 'Shortcuts' screen.

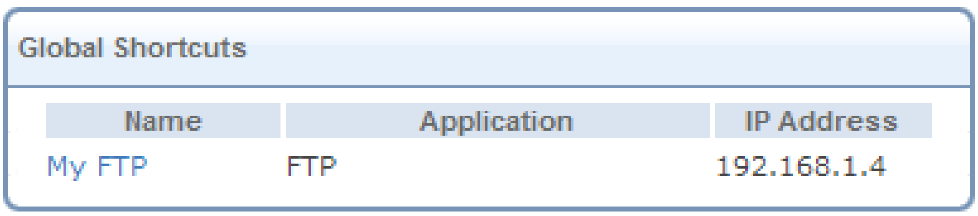


Figure 5.325 Shortcut to FTP

5.8.2.2.5 Telnet

This option enables the user to connect and perform tasks on a computer inside OpenRG's LAN with the Telnet application. In the 'Shortcut Wizard' screen, configure the following parameters.

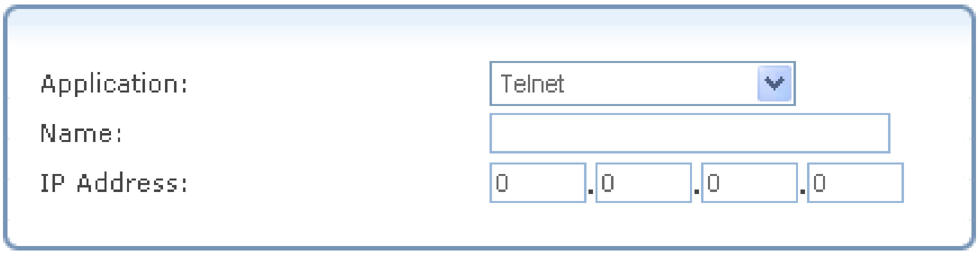


Figure 5.326 Telnet Parameters

Name Enter a name for this shortcut.

IP Address Enter the IP address of the LAN computer on which to perform the application.

Once you configure a shortcut to Telnet and associate it with a user (or group), you can use the application when logged into the SSL VPN portal as that user, by clicking the shortcut link that appears in the 'Shortcuts' screen.

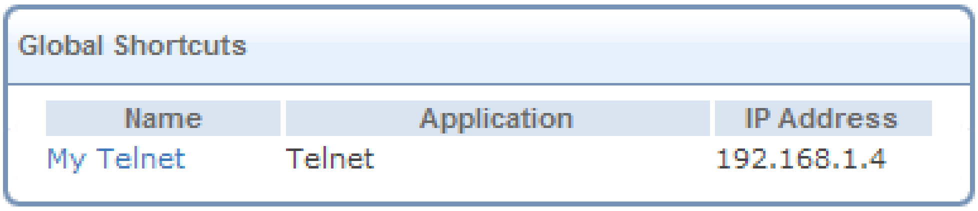


Figure 5.327 Shortcut to Telnet

5.8.2.3 Accessing and Using the SSL VPN Portal

The SSL VPN portal is accessible from within OpenRG for administration purposes, by clicking the 'SSL-VPN Portal' link in the 'SSL-VPN' screen (see Figure 5.299).

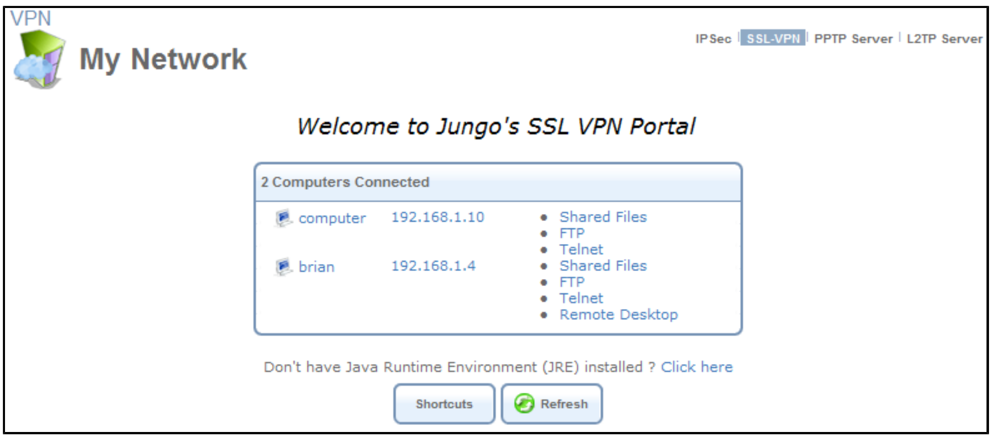


Figure 5.328 SSL VPN Portal Viewed from OpenRG

However, its purpose is to serve as an administrative portal for remote users who log into OpenRG from the Internet via HTTPS. To log in as a remote user, browse to OpenRG from a remote computer by typing **https://<OpenRG's Internet address>** (OpenRG's Internet address can be found under the 'Internet Connection' tab). For example, **https://10.71.86.21**. You will be required to provide the login details of the remote user with which you would like to connect.

The initial SSL VPN screen refreshes as OpenRG detects the open ports of each host, displaying links to applications (services) associated with these ports. This auto-detection utility is available in addition to the global shortcuts mechanism.

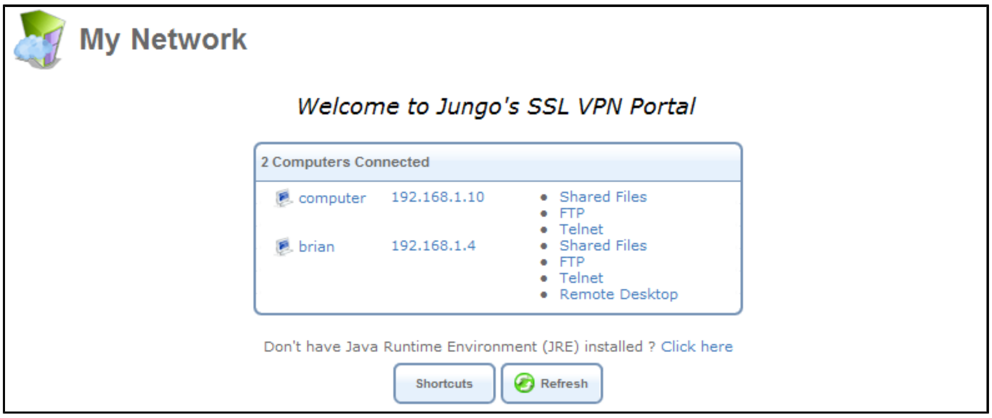


Figure 5.329 SSL VPN Portal Viewed from the Internet

Click a host name or IP address to view its information.

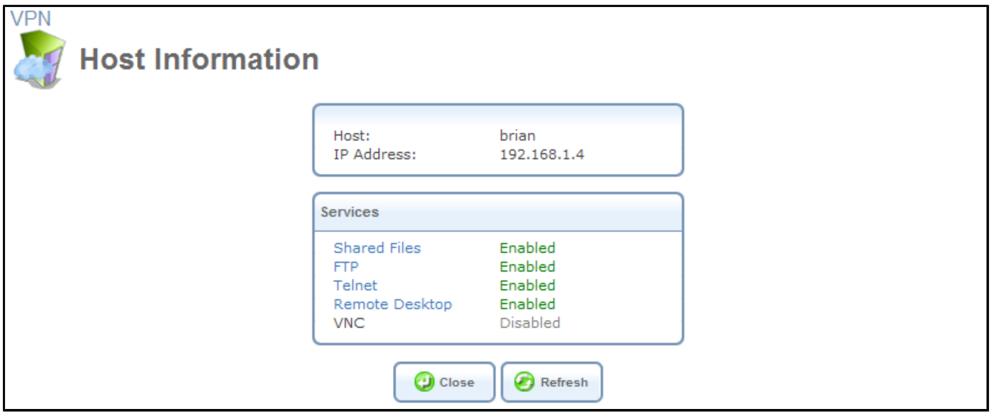


Figure 5.330 Host Information

When clicking an application link in the 'Services' section, OpenRG will attempt to use the login details of the logged-in user (in case the application requires a username and password).

> Note: All available applications require the Java Runtime Environment (JRE) to be available on the remote computer. Use the "Click here" link at the bottom of the SSL VPN portal screen to install this environment.

Click 'Close' to return to the SSL VPN portal.

Global shortcuts are predefined with all the necessary parameters (including login details where required) to ensure a reliable application launch. Click the 'Shortcuts' button to view the available global shortcuts.

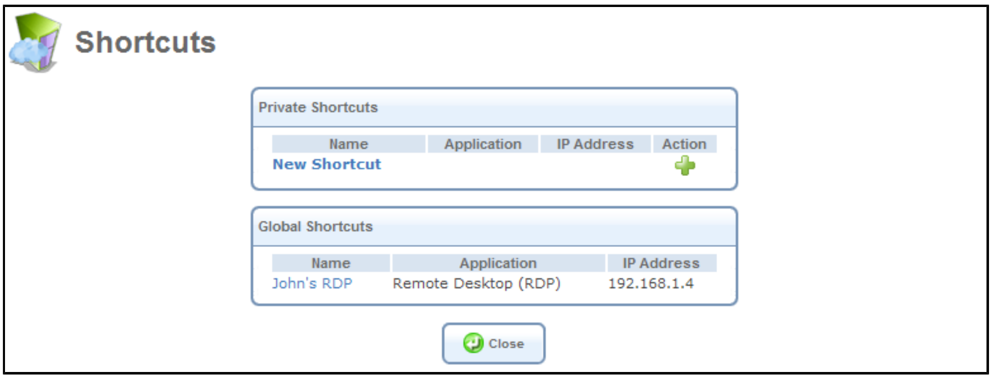


Figure 5.331 Shortcuts

5.8.2.3.1 Creating a Private Shortcut

In addition to the global shortcuts, each user can use the SSL-VPN portal to configure private shortcuts, displayed only for him when logged in. To add a new private shortcut, perform the following:

1. In the 'Private Shortcuts' section of the 'Shortcuts' screen, click the 'New Shortcut' link. The 'Shortcut Wizard' screen appears. This process is identical to the addition of a global shortcut.

2. After configuring the application parameters, click 'Next'. The following wizard screen appears.

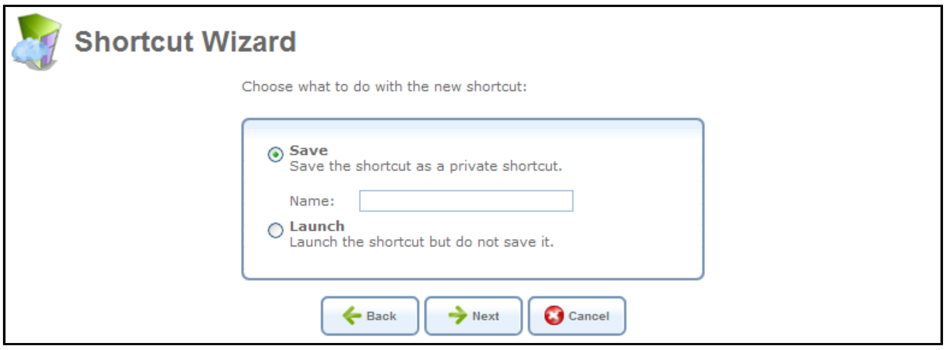


Figure 5.332 Save or Launch

3. You can either save the private shortcut or launch it without saving. Select a radio button and click 'Next'. The 'Shortcut Summary' screen appears.

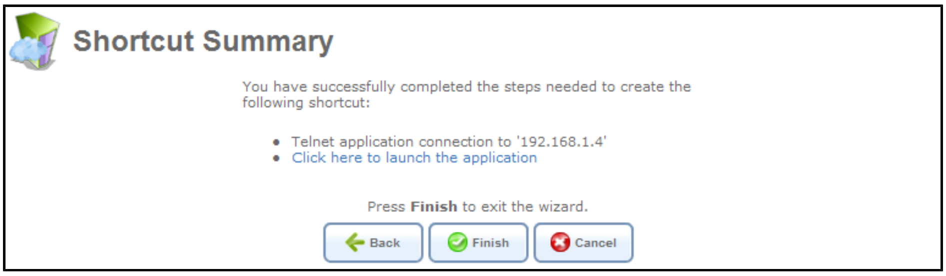


Figure 5.333 Launch

4. If you chose "Launch", click the provided link. Otherwise, click 'Finish'. The new shortcut is added to the 'Private Shortcuts' section of the 'Shortcuts' screen, and will be available exclusively for this user when connecting to the SSL VPN portal.

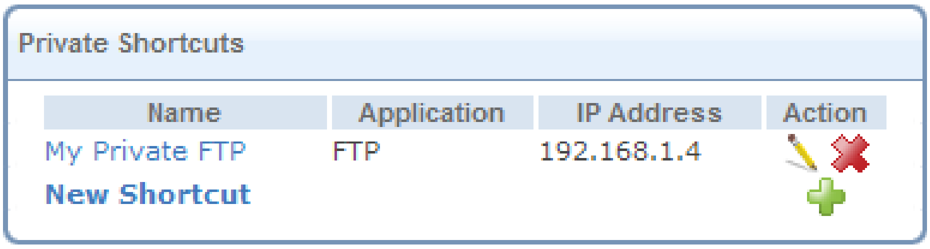


Figure 5.334 Private Shortcuts

5.8.2.3.2 Customizing the SSL VPN Portal

You can customize the look and the behavior of the SSL VPN portal from the 'SSL VPN' screen.

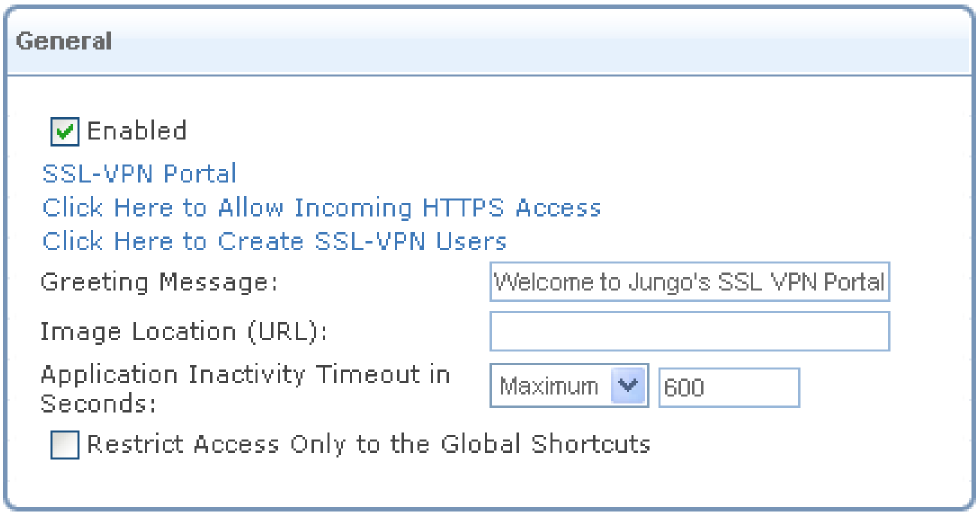


Figure 5.335 SSL VPN

Greeting Message Enter the greeting message that will appear at the top of the SSL VPN portal screen.

Image Location (URL) Enter the URL of an image you would like to display at the top-left of the portal screen (instead of the default image).

Application Inactivity Timeout in Seconds The timeframe of application idleness in seconds, after which the application disconnects. The user will have to use the shortcut to reactivate the application. Enter zero if you would like to un-limit this timeframe.

Restrict Access Only to the Global Shortcuts When checked, only the global shortcuts will appear and be accessible.

5.8.3 Point-to-Point Tunneling Protocol Server

OpenRG can act as a Point-to-Point Tunneling Protocol Server (PPTP Server), accepting PPTP client connection requests.

5.8.3.1 Configuring the PPTP Server

Access this feature either from its link in the 'VPN' tab under the 'Services' screen, or by clicking the 'PPTP Server' icon in the 'Advanced' screen. The 'Point-to-Point Tunneling Protocol Server (PPTP Server)' screen appears:

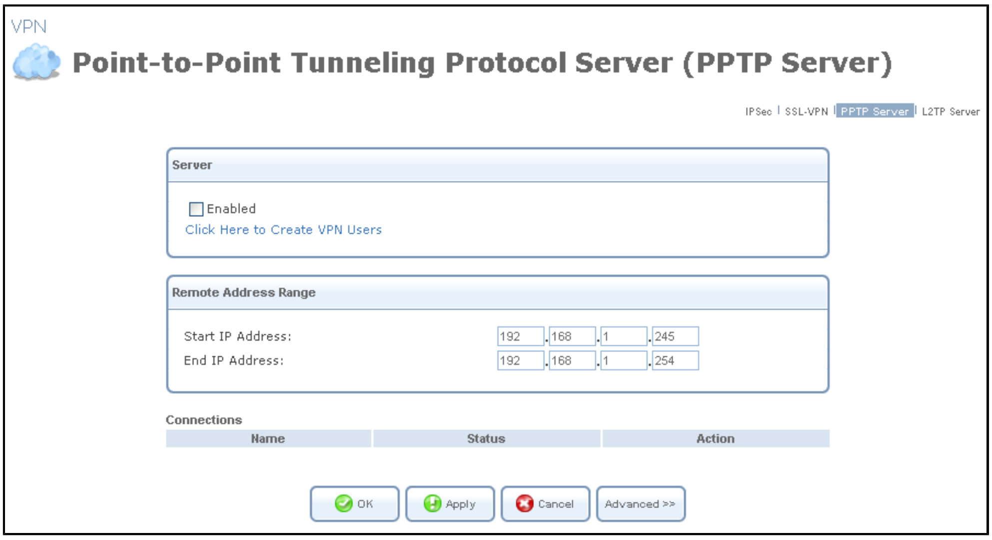


Figure 5.336 Point-to-Point Tunneling Protocol Server (PPTP Server)

This screen enables you to configure:

Enabled Select or deselect this check box to enable or disable this feature.
Note that checking this box creates a PPTP server (if not yet created with the wizard), but does not define remote users.

Click Here to Create VPN Users Click this link to define remote users that will be granted access to your home network. Refer to Section 6.3 to learn how to define and configure users.

Remote Address Range Use the 'Start IP Address' and 'End IP Address' fields to specify the range of IP addresses that will be granted by the PPTP server to the PPTP client.

5.8.3.2 Advanced PPTP Server Settings

To configure advanced PPTP server settings press the 'Advanced' button on the PPTP screen (see Figure 5.336). The screen expands, offering additional settings:

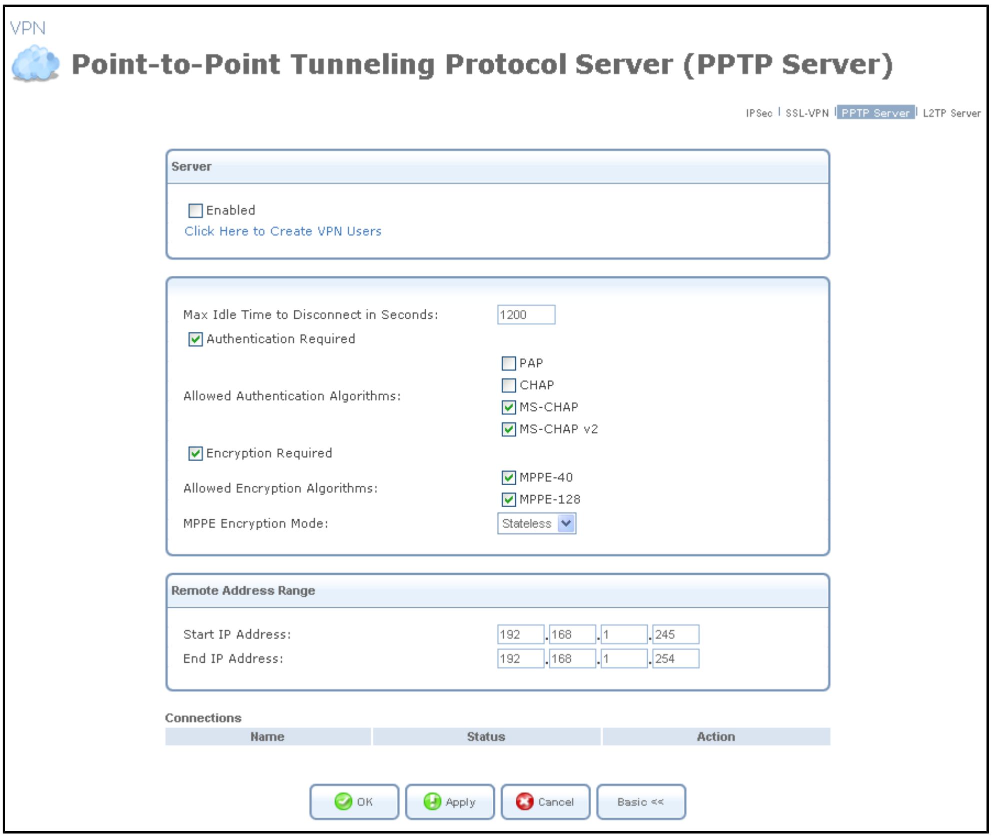


Figure 5.337 Advanced PPTP Server Parameters

Maximum Idle Time to Disconnect in Seconds Specify the amount of idle time (during which no data is sent or received) that should elapse before the gateway disconnects a PPTP connection.

Authentication Required Select whether PPTP will use authentication.

Allowed Authentication Algorithms Select the algorithms the server may use when authenticating its clients.

Encryption Required Select whether PPTP will use encryption.

Allowed Encryption Algorithms Select the algorithms the server may use when encrypting data.

MPPE Encryption Mode Select the Microsoft Point-to-Point Encryption mode: stateless or stateful.

Note that the server settings must be in tune with the client settings, described in Section 6.4.11.

5.8.4 Layer 2 Tunneling Protocol Server

OpenRG can act as a Layer 2 Tunneling Protocol Server (L2TP Server), accepting L2TP client connection requests.

5.8.4.1 Configuring the L2TP Server

Access this feature either from the 'VPN' menu item under the 'Services' tab, or by clicking the 'L2TP Server' icon in the 'Advanced' screen. The 'Layer 2 Tunneling Protocol Server (L2TP Server)' screen appears.

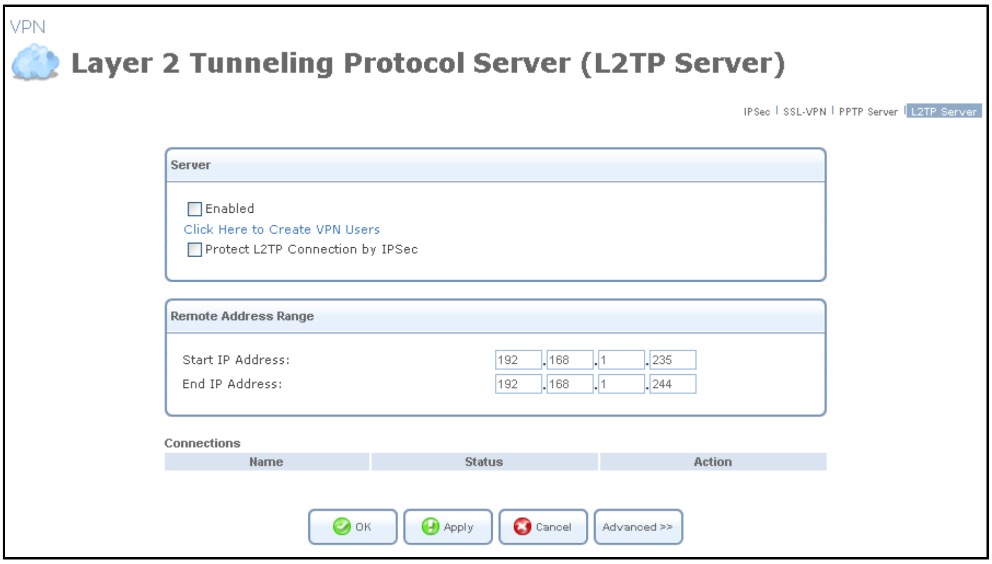


Figure 5.338 Layer 2 Tunneling Protocol Server (L2TP Server)

This screen enables you to configure the following connection settings:

Enabled Select or deselect this check box to enable or disable this feature.
Note that selecting this box creates an L2TP server (if not yet created with the wizard), but does not define remote users.

Click Here to Create VPN Users Click this link to define remote users that will be granted access to your home network. Refer to Section 6.3 to learn how to define and configure users.

Protect L2TP Connection by IPSec By default, the L2TP connection is not protected by the IP Security (IPSec) protocol. Select this option to enable this feature. When enabled, the following entry appears.

Create Default IPSec Connection When creating an L2TP Server with the connection wizard, a default IPSec connection is created to protect it. If you wish to disable this feature, uncheck this option. However, note that if L2TP protection is enabled by IPSec (see previous entry), you must provide an alternative, active IPSec connection in order for users to be able to connect. When this feature is enabled, the following entry appears.

L2TP Server IPSec Shared Secret You may change the IPSec shared secret, provided when the connection was created, in this field.

Remote Address Range Use the 'Start IP Address' and 'End IP Address' fields to specify the range of IP addresses that will be granted by the L2TP server to the L2TP client.

5.8.4.2 Advanced L2TP Server Settings

To configure advanced L2TP server settings, click the 'Advanced' button in the L2TP Server screen (see Figure 5.338). The screen expands, offering additional settings.

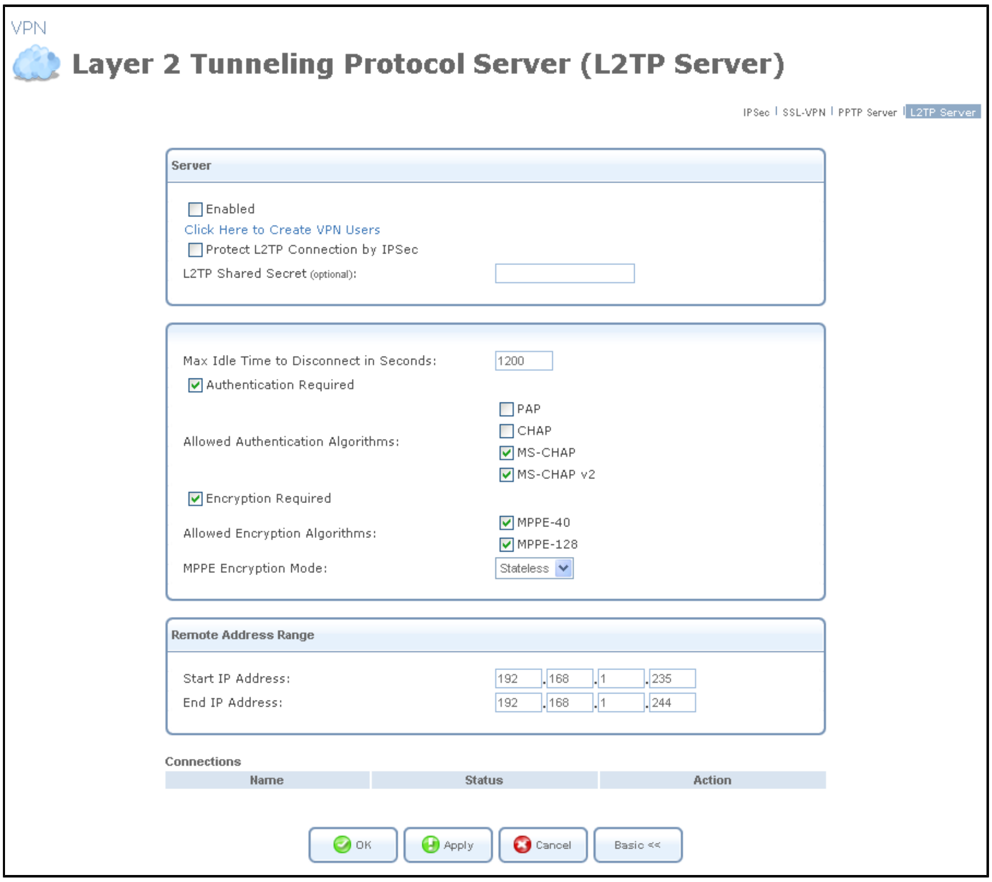


Figure 5.339 Advanced L2TP Server Parameters

L2TP Shared Secret (optional) Use this optional field to define a shared secret for the L2TP connection, for added security.

Maximum Idle Time to Disconnect in Seconds Specify the amount of idle time (during which no data is sent or received) that should elapse before the gateway disconnects the L2TP connection.

Authentication Required Select whether L2TP will use authentication.

Allowed Authentication Algorithms Select the algorithms the server may use when authenticating its clients.

Encryption Required Select whether L2TP will use encryption.

Allowed Encryption Algorithms Select the algorithms the server may use when encrypting data.

MPPE Encryption Mode Select the Microsoft Point-to-Point Encryption mode: stateless or stateful.

5.8.4.3 Configuring an L2TP over IPSec VPN Client

If you wish to connect to OpenRG's L2TP server (with the default IPSec configuration) using the Windows IPSec client, configure your host's L2TP connection with the following:

- Your login credentials (for more information, refer to Section 6.3)
- The L2TP server's IPSec shared secret (for more information, refer to Section 5.8.4.1).
- The L2TP server's IP address (OpenRG's WAN address)

In case you wish to use a third-party IPSec client (for example, Netscreen) with your L2TP connection, configure the client with the following parameters. Note that these parameters match the gateway's default IPSec VPN connection parameters.

Remote Party's Identity

- **ID Type** Select 'IP Address', and specify OpenRG's WAN IP address.
- **Protocol** Select UDP.
- **Port** Select L2TP 1701.

My Identity

- **ID Type** Select 'IP Address'.
- **Port** Select L2TP 1701.

Security Policy Select the 'Main' mode.

Phrase 1 Negotiation Mode

- Select 'IPSec Shared Secret' as the peer authentication method, and enter the shared secret defined in the L2TP server's IPSec VPN settings.
- Define the encryption algorithm—by default, OpenRG supports the 3DES-CBC algorithm.
- Define the hash algorithm—OpenRG supports both the MD5 and SHA1 algorithms.
- Define the Key group—by default, OpenRG supports Diffie-Hellman (DH) Group 2 and Group 5.

Phrase 2 Negotiation Mode

- Enable the 'Encapsulation Protocol' option.
- Define the encryption and hash algorithms exactly as in Phase 1.
- Set the encapsulation method to 'Transport'.

5.9 Storage

5.9.1 FTP Server

OpenRG can operate as a File Transfer Protocol (FTP) server, allowing users and guests to access its internal disks, to easily (but securely) exchange files. OpenRG's FTP access consists of two levels:

- User Access Registered users can access predefined directories, which are protected by their username and password.
- Anonymous Access Guests can access predefined public directories. This feature allows you, for example, to let guests download a certain file.

5.9.1.1 User Access FTP

To configure an FTP user, perform the following:

1. Click the 'Users' icon in the 'Advanced' screen of the management console. The 'Users' screen appears.

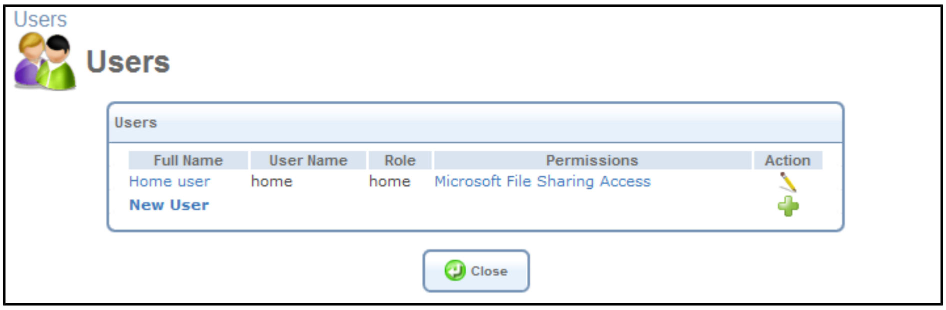


Figure 5.340 Users

2. Click the edit icon of the user for which you would like to grant FTP access. The 'User Settings' screen appears.

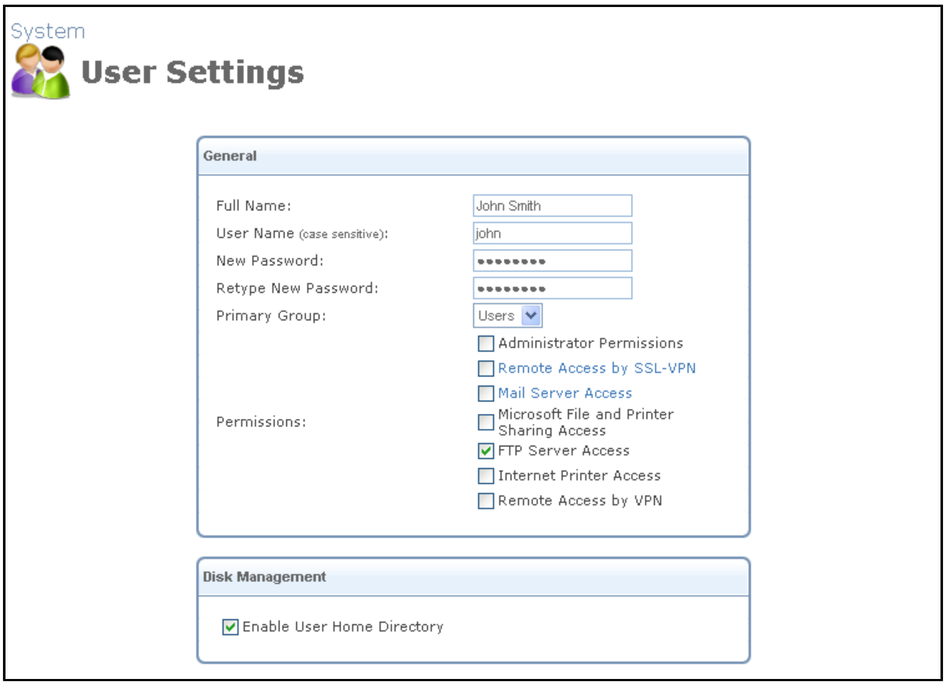


Figure 5.341 User Settings

3. In this screen, perform the following:

    1. In the Permissions section, check the 'FTP Server Access' check box, to grant this permission.

    2. Check the 'Enable User Home Directory' check box. This feature creates a home directory for the user.

4. Click 'OK' to save the settings.

5. Access the FTP Server settings either from the 'Storage' tab under the 'Services' screen, or by clicking the 'FTP Server' icon in the 'Advanced' screen. The 'FTP server' screen appears. Check the 'Enabled' check box to view the full FTP screen.

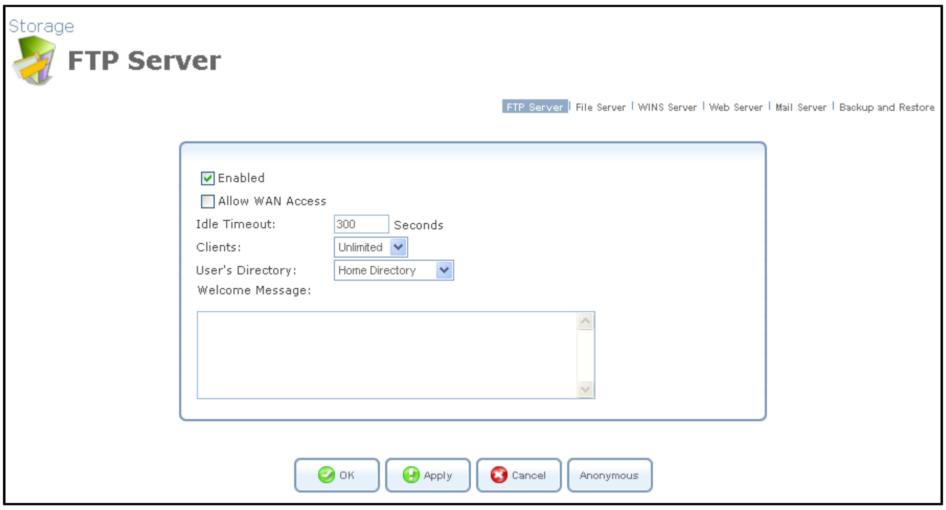


Figure 5.342 Enabled FTP Server

6. In this screen, perform the following:

    1. Check the 'Allow WAN Access' check box if you wish to allow registered users to use the FTP from the WAN.

    2. Enter the maximum number of seconds that a user may spend between FTP commands before the session times out, in the 'Idle Timeout' field. This setting is global for all users, both registered and guests.

    3. Choose the maximum number of users that can use the FTP simultaneously. You can choose between "Unlimited" and "Maximum" in the 'Clients' combo box. When choosing 'Maximum', a second field appears allowing you to enter the number of users. This setting is also global.

    4. In the 'User's Directory' combo box, choose 'Home Directory' to allow registered users to access their home directories. Alternatively choose 'Common Directory'. A second field will appear in which you should specify a common directory relative to '<User Data>/'. All registered users will be able to access this directory only.

    5. Enter a welcome message that will be displayed for all users after logging in (optional).

7. Click 'OK' to save the settings.

5.9.1.2 Anonymous Access FTP

To configure an anonymous or guest FTP user, perform the following:

1. Click the 'Anonymous' button at the bottom of the 'FTP Server' screen (see Figure 5.342). The 'Anonymous Access' screen will appear (see Figure 5.343).

2. Check the 'Allow LAN/WAN Access' check boxes to allow guests FTP access to the LAN or the WAN, or both. A second field appears labeled 'LAN/WAN Root Directory'. The default directory is { home/ftp}, which is OpenRG's pre-configured directory with guest permissions and the usernames "ftp" and "anonymous" (any passwords will be accepted).

Figure 5.343 Anonymous Access

3. Click 'OK' to save the settings.

Note: The FTP Server assumes that any path or directory that you enter during the configuration exists. Each file in the directory should have the correct permissions for the relevant user. Files in the anonymous directories should have the relevant permissions for the built-in 'ftp' user.

5.9.2 Managing Your File Server

OpenRG provides a file server utility, allowing you to perform various tasks on your files, such as manage file server shares and define access control lists. When a mass storage device is connected to the gateway, all disk partitions are automatically shared by default.

Access the file server settings by clicking the 'Storage' menu item under the 'Services' tab. The 'File Server' screen appears.

Figure 5.344 File Server

Enabled Select or deselect this check box to enable or disable this feature.

NetBIOS Workgroup OpenRG's workgroup name that will be displayed in the Windows network map of LAN hosts. All computers connected to OpenRG's network will appear in this workgroup.

Automatically Share All Partitions A partitioned storage device connected to OpenRG is automatically displayed and shared by all LAN computers. This feature is enabled by default.

Allow Guest Access From the drop-down menu, select a permission level, according to which the LAN users will access the share:

Read/Write Every LAN user can read and write the shared files without authentication.

Read Only Every LAN user can only read the shared files.

Disabled LAN users must authenticate themselves, in order to access the share. They will be able to use the share according to their permissions defined in OpenRG's 'User Settings' screen.

File Server Shares Define file shares on your disk partitions, as depicted in the following sections.

5.9.2.1 Sharing Specific Partitions with Microsoft File Sharing

By default, all partitions are automatically displayed shared among all users. Figure 5.344 depicts such a scenario, where share entries appear in the 'File Server Shares' section as soon as a partitioned and formatted storage device is connected to the gateway. However, if you only wish to share specific partitions, you can disable automatic file sharing and manually define file shares using the 'Microsoft File Sharing Protocol'. Note that this protocol requires associating specific users with the shares.

To share a specific partition only, perform the following sequence. First, enable Microsoft File Sharing for users you would like to have access to the share:

1. Click the 'Users' menu item under the 'System' tab. The 'Users' screen appears.

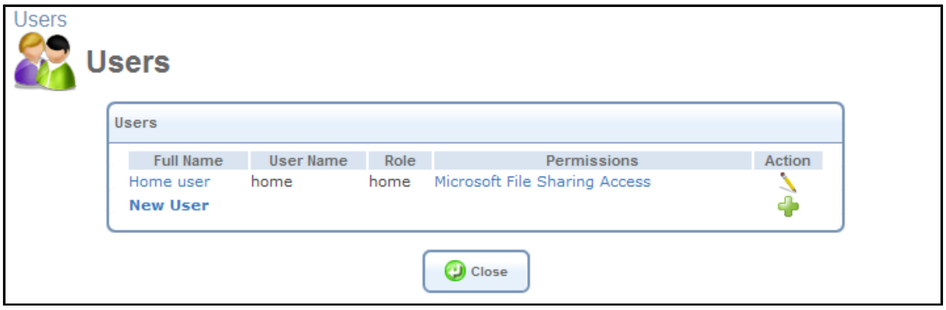


Figure 5.345 Users

2. Click the name of the user for whom you wish to enable file sharing.

3. In the 'User Settings' screen that appears, check the "Microsoft File and Printer Sharing Access" check box in the 'Permissions' section.

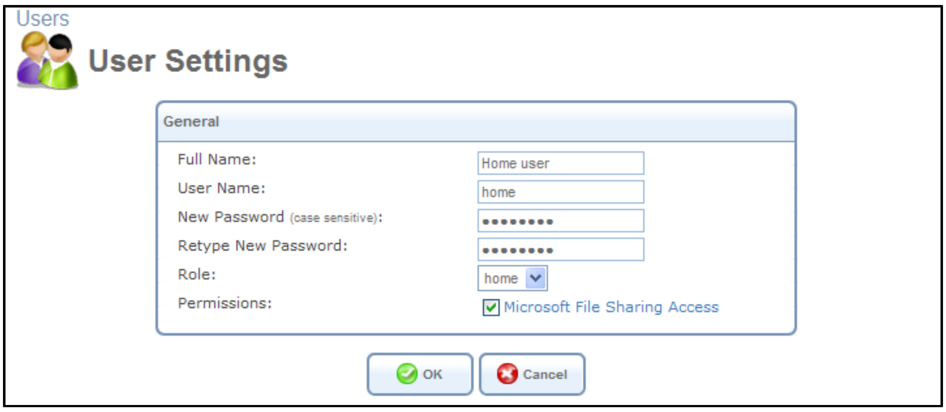


Figure 5.346 User Settings

4. Click 'OK' to save the settings.

Next, define the specific file share:

1. In the 'File Server' screen (see Figure 5.344), deselect the 'Automatically Share All Partitions' option and click 'Apply'. The list of all automatically shared partitions disappears.
2. Click the 'New Entry' link. In the 'File Server Share Settings' that appears:
    a. Enter a name for the share in the 'Name' field.

> Note: The default name "share" can be changed to another one. The share's name is not case sensitive. Even if entered in upper-case letters, the name will be displayed in lower case, after saving the setting.

    b. Enter a valid partition path (e.g. A, B/my_documents) in the 'Path' field.

> Note: If a drive's sub directory does not exist yet, you will have to create it as soon as the share is defined and accessible.

    c. You may add a comment in the 'Comment' field.

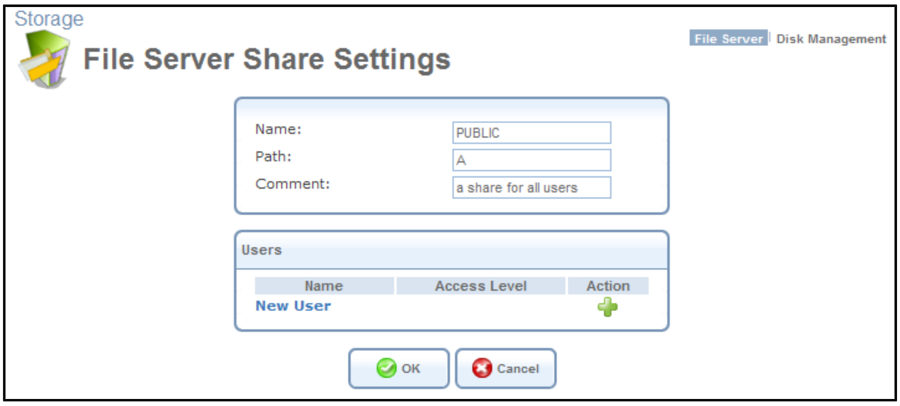


Figure 5.347 File Server Share Settings

    d. In the 'Users' section, click the 'New User' link to allow a user to use the share.

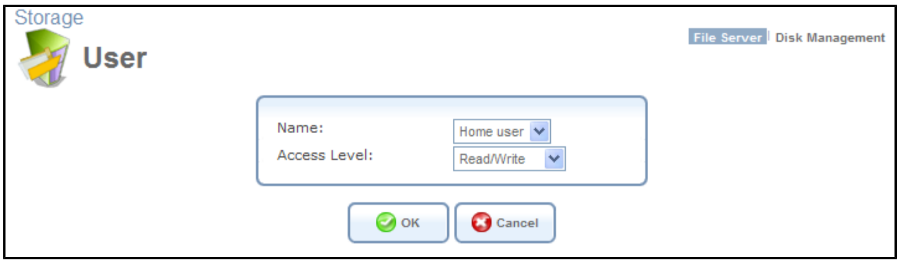


Figure 5.348 User

    e. Select the user and the allowed access level in the drop-down menus, and click 'OK'.

3. Click 'OK' to save the settings. The 'File Server' screen reappears, displaying the share in the 'File Server Shares' section.

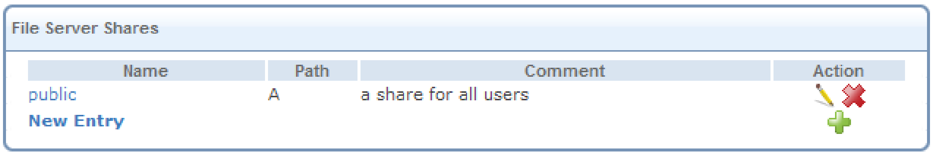


Figure 5.349 File Server Shares Section

However, note that access to a file share is different for FAT32, NTFS, and EXT2/3 formatted partitions. FAT32 has no restrictions—any user can access any share for both reading and writing. However, the data stored on NTFS partitions is only readable (unless OpenRG is based on the Conexant Solos or Freescale platforms).

In addition, shares defined on EXT2/3 partitions are only readable to non-administrator users (even with writing permissions), with the following exceptions:

- The user will be able to write to the share's root directory (e.g. A\, my_share\).
- The user will be able to write to his/her home directory, if such had been created for that user, by enabling the 'Enable User Home Directory' option in the 'User Settings' screen (see Figure 5.346).

Moreover, to create new directories that will be writable for users, you must be logged in as a user, not an administrator. Any directories created by an administrator will only be writable to the administrator.

To access the new share, you must be logged in with a user associated with share (in this example, user 'home'). Perform the following:

1. Click the share's link under the 'Name' column in the 'File Server Shares' section (see Figure 5.349).

> Note: If the share is not available, for example if the disk has been removed, the link will not be clickable and appear as plain text.

A Windows login dialog box appears.

Figure 5.350 Login Dialog

2. Enter your WBM username and password to login. The share opens in a new window.

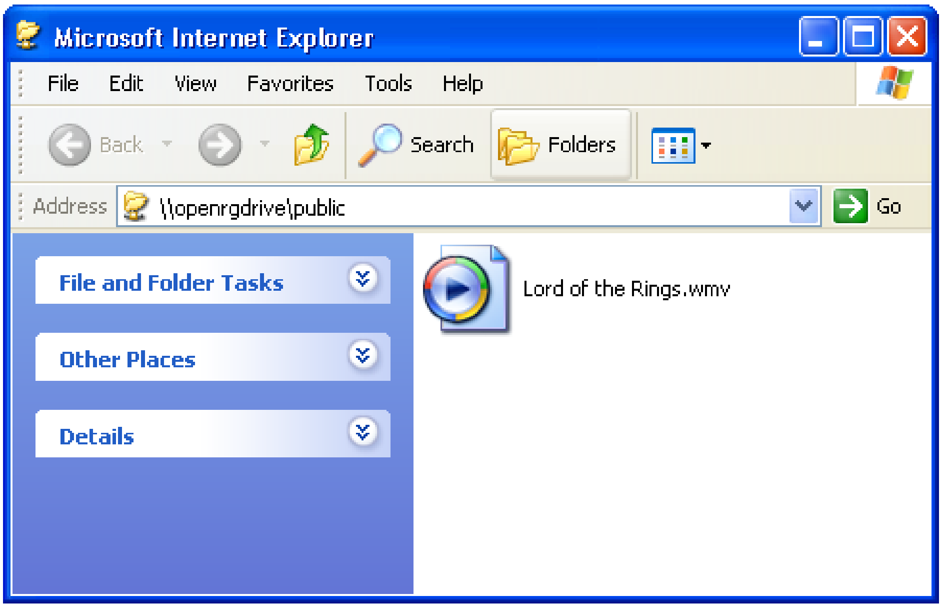


Figure 5.351 File Share

Once logged into a share, Windows remembers your username and password, and automatically re-logins with the same user. To logout and re-login with a different user (for example, to switch between an administrator and a user), logout and re-login to Windows.

Users with appropriate permissions can access file shares from any PC on the LAN using the following standard methods:

- From OpenRG's Web-based management as described above.
- Browsing to the share itself by simply typing its path (for example, openrg\A) in a browser address line or in the command line.
- Mapping the share using Window's 'Map Network Drive' utility.

All of these methods require an initial username and password login, as described above. The share content will be displayed in a new window. If the share is the partition configured to serve as the system storage area, it will contain automatically-generated system folders. Otherwise, it will either be empty or contain pre-loaded files.

5.9.2.2 Viewing and Modifying Access Control Lists

The Windows operating system boasts an extensive file permission scheme. When you right-click a file and choose Properties, you can see under the Security tab (see Figure 5.352) that file permissions can be defined for any number of users and groups. Each user and group may be allowed or denied several levels of access, ranging from Full Control to Read only.

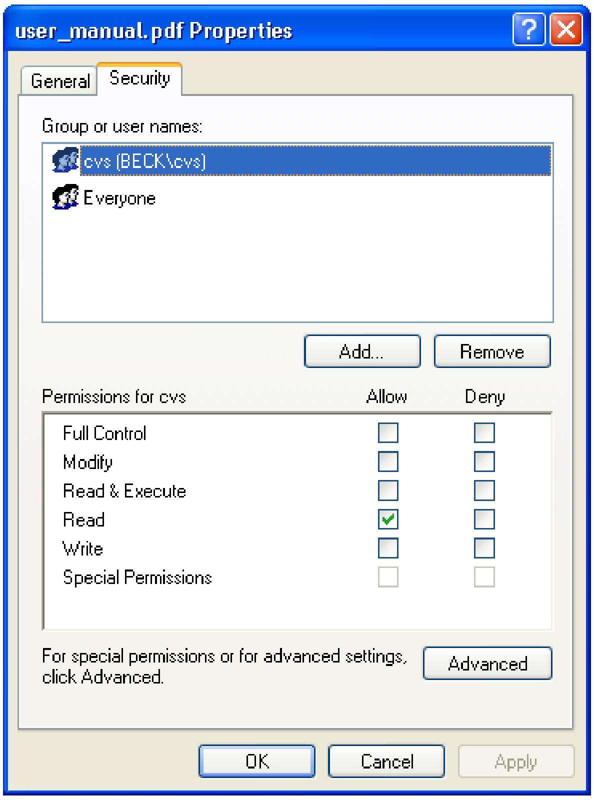


Figure 5.352 File Properties

Linux, on the other hand, has a very limited file permissions scheme, offering the basic Read (r), Write (w) and Execute (x) permissions to the file owner and his group only. Access Control Lists (ACLs) are an extension of the common Linux permission scheme. ACLs allow granting the aforementioned permissions not only to the file owner and his group, but to any number of users and groups. The need for ACLs in OpenRG is mainly to support permissions defined by a Windows client connected to the file server. This connection is done via the 'Microsoft File and Printer Sharing Protocol', which is supported on OpenRG and allows interoperability between Linux/Unix servers and Windows-based clients. The basic user and group file permissions in Windows are: Full control, Modify, Read and Execute, Read, and Write. Each permission can be allowed or denied. Linux supports Read, Write and Execute only, and does not support the Allow/Deny mechanism. When you modify a file's permissions on a Windows client, OpenRG uses a "best effort" algorithm to translate the ACLs to Linux r/w/x bits, making the file compatible with Linux clients.

To view a file's access control list on a Windows client connected to OpenRG's file server, perform the following:

1. Click the file share link in the 'File Server Shares' section (see Figure 5.349) of the 'File Server' screen to open the file share (login with a valid user for the share if a login prompt appears).
2. Create a file on the share.
3. Right-click the file and choose "Properties".
4. Click the Security tab to view the file ACLs (see Figure 5.352). If you do not have a Security tab:
    1. Open "My Computer" and choose Tools and then Folder Options.
    2. Under the View tab, uncheck the "Use simple file sharing (Recommended)" check box.

Under the Security tab you can view the permissions of the file owner, the owner's group and the group "Everyone", for all other users. If you have more users (or groups) defined on OpenRG, you can add them to the file's ACL and grant them permissions. To modify a file's access control list, perform the following:

1. Click the 'Add' button in the Security tab window to view the users and groups list.
2. In the 'Select Users or Groups' window that appears (see Figure 5.353), press the 'Advanced' button.

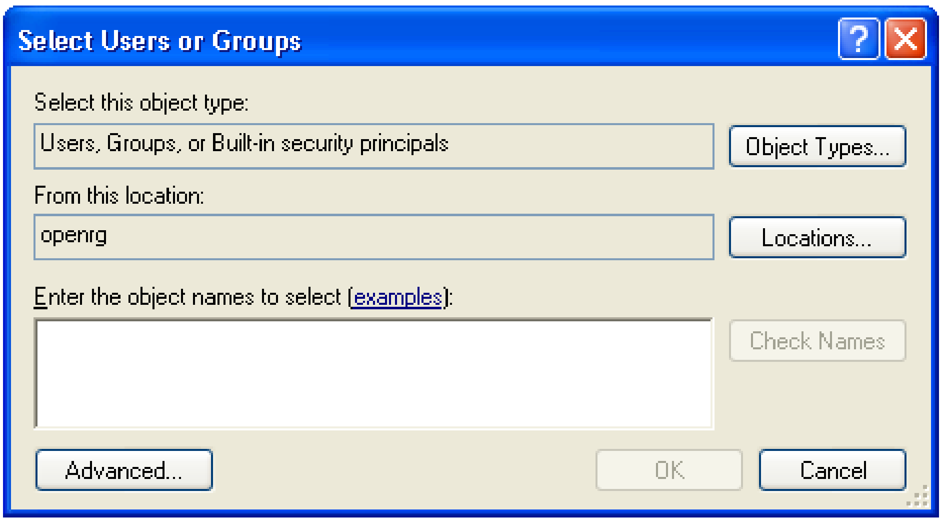


Figure 5.353 Select Users or Groups

3. In the advanced window (see Figure 5.354) press the 'Find Now' button.
4. A login prompt will appear. Log in with the same share user [1]. A list of both OpenRG users and system default users will be displayed.

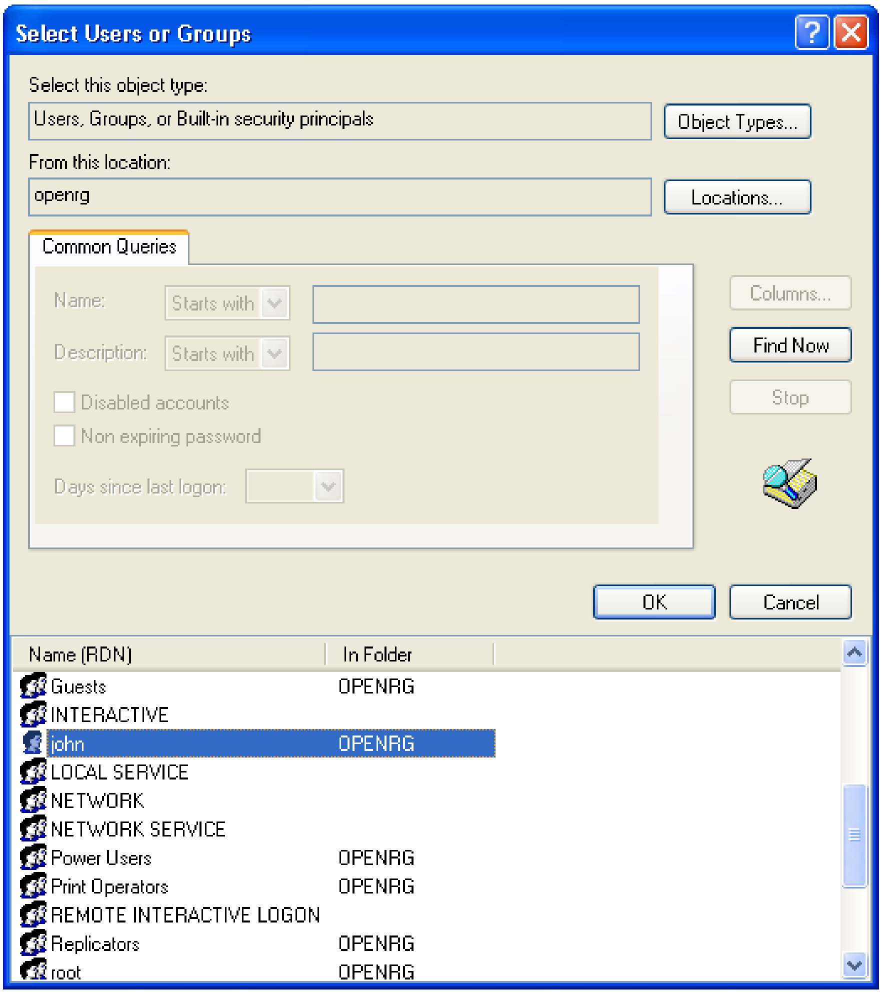


Figure 5.354 Users or Groups List

5. Select an OpenRG user from the list and click 'OK'. Click 'OK' again in the initial 'Select Users or Groups' window to save the settings. The selected user will be added to the groups and users list on the Security tab, with the default ACLs.

6. Check or uncheck the different permissions to allow or deny the user of the permissions.

7. Click 'OK' to save the settings.

In the same manner, you can remove a user or a group using the 'Remove' button in the Security window.

5.9.2.3 Using the File Server with Mac

In order to connect to OpenRG's file server with a Mac computer, perform the following:

1. On your Mac computer connected to OpenRG, click "Connect to Server" from the "Go" menu. The 'Connect to Server' screen appears.

Figure 5.355 Connect to Server

2. In the server address field, enter **smb://192.168.1.1** , and click the 'Connect' button. A new window appears, displaying the available file shares.

Figure 5.356 Connect to Server

3. Select the share to which you would like to connect. If prompted, enter a valid username and password, and click 'OK'. When a connection is established, the share content appears.

Figure 5.357 Connect to Server

5.9.3 WINS Server

OpenRG can operate as a Windows Internet Naming Service (WINS) server, handling name registration requests from WINS clients and registering their names and IP addresses. WINS is a name resolution software from Microsoft that converts NetBIOS names to IP addresses.

Windows machines that are named as PCs in a workgroup rather than in a domain use NetBIOS names, which must be converted to IP addresses if the underlying transport protocol is TCP/IP. Windows machines identify themselves to the WINS server, so that other Windows machines can query the server to find the IP address. Since the WINS server itself is contacted by IP address, which can be routed across subnets, WINS allows Windows machines on one LAN segment to locate Windows machines on other LAN segments by name. When a host connects to the LAN, it is assigned an IP address by OpenRG's DHCP (refer to Section 5.11). The WINS database is automatically updated with its NetBIOS name and the assigned IP address. OpenRG's WINS server also responds to name queries from WINS clients by returning the IP address of the name being queried (assuming the name is registered with the WINS server). The "Internet" in the WINS name refers to the enterprise Internet (LAN), not the public Internet. To configure OpenRG's WINS server settings, perform the following:

1. Access the WINS Server settings either from its link in the 'Storage' tab under the 'Services' screen, or by clicking the 'WINS Server' icon in the 'Advanced' screen. The 'WINS Server' screen will appear (see Figure 5.358). By default, OpenRG's WINS server is disabled.

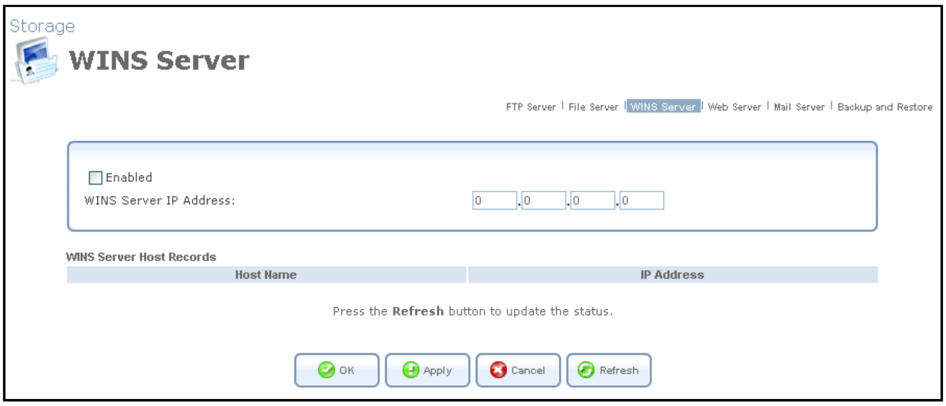


Figure 5.358 WINS Server

2. If you would like to use an external WINS server, enter its IP address and click 'OK'.

3. If you would like to use OpenRG's WINS server, select the 'Enabled' check-box. The screen will refresh, omitting the IP address field (see Figure 5.359).

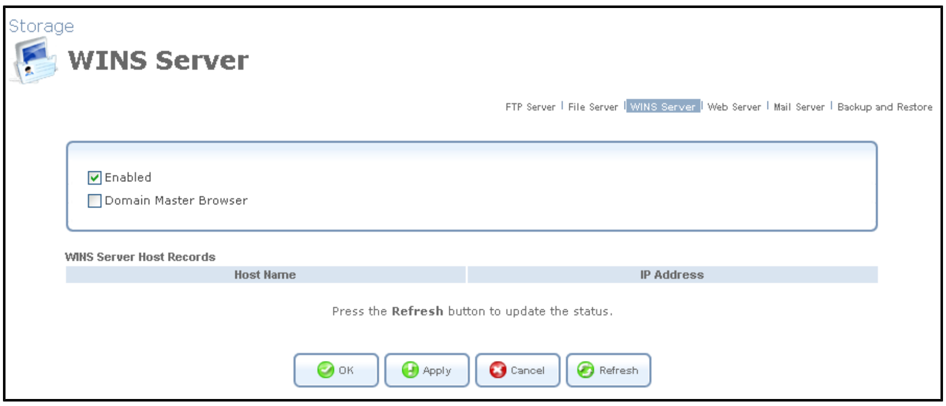


Figure 5.359 WINS Server

4. Select the 'Domain Master Browser' check box if you would like OpenRG to act as a domain master in the Windows NetBIOS protocol.

5. Click 'OK' to save the settings.

Hosts connected to the LAN will register their names and IP addresses with either the specified remote WINS server or with OpenRG's WINS server, depending on the configuration above. In both cases, the registered hosts will be added to the 'WINS Server Host Records' table in this screen.

5.9.4 Web Server

OpenRG can operate as a Web server, hosting one or more Web sites which are accessible from the LAN or the WAN. The advantages of this feature are:

- The Web site is hosted on OpenRG, eliminating the need to assign a station on the LAN to act as a Web server, or to outsource expensive hosted services.
- LAN security: users from the Internet can access your Web site without entering your LAN.
- Simple and fast configuration.

There are several preliminary actions that you must take before configuring your Web server on OpenRG:

1. Register a domain name and map it to OpenRG's WAN IP (refer to Section 5.10).

2. Connect a storage device (such as a hard drive) to OpenRG and configure its file server (refer to Section 5.9.2).

3. Verify that the System Storage Area is configured, as described in Section 5.9.7.2.

4. Create your Web files, and upload them to a folder on the file server.

> Note: It is important that you name the Web site's homepage **index.html** or **index.htm**, and upload it to the file server.

Access the Web server settings either from its link under the 'Storage' menu item of the 'Services' tab, or by clicking the 'Web Server' icon in the 'Advanced' screen. The 'Web Server' screen appears.

Figure 5.360 Web Server

Enabled Select or deselect this check box to enable or disable this feature.

WAN Access Select this check box to allow access to your Web server over the Internet.

Log Requests Select this check box to log connection requests sent to your Web server.

HTTP Port The port your Web server uses for HTTP traffic.

HTTPS Port The port your Web server uses for HTTPS traffic.

Note: The default HTTP and HTTPS ports may be used by another service. In this case, reconfigure either this service or the Web server with unoccupied port numbers. For example, as the WBM by default uses HTTP port 80, it will disconnect after activating the Web server. To access it again, either change the Web server's default HTTP port, or browse to the WBM with an alternative port—for example, **http://192.168.1.1:82**.

The following sections describe how to configure OpenRG's Web server capabilities, including hosting user-private Web pages and multiple independent Web sites.

5.9.4.1 Setting Up Your Web Site on OpenRG

1. In the 'Data Location' field of the 'Web Server' screen, enter the file system path of the OpenRG folder containing your Web site's content.

Figure 5.361 Data Location Field

2. Click 'OK' to save the settings.

5.9.4.2 Hosting User Private Web Pages

Each user on the LAN can configure a private Web page, which can be reached by browsing to http://openrg.home/~<username>. This path will be mapped to a sub directory of the users' home directory on OpenRG.

To set a private Web page:

1. Verify that the 'User Home Directory' option is enabled in the user's account settings screen (for more information, refer to Section 6.3.4).
2. In the 'User Private Web Page' section of the 'Web Server' screen, select the 'Enabled' check box.
3. In the 'Data Location' field, enter the user's sub directory containing the Web site's content.

Figure 5.362 User Private Web Page

4. Click 'OK' to save the settings.

5.9.4.3 Setting Up Virtual Hosts on OpenRG

You can configure any number of additional Web sites on the OpenRG Web server. Each of these sites will appear to the Internet user as if they are located on separate hosts. This method is referred to as *Virtual Hosts*. In addition, you can add any number of aliases to each virtual host. Browsers from within the LAN will reach your Web sites directly. However, to provide external access to your sites, you will have to register domain names. These domain names must be mapped to OpenRG's WAN IP address by the DNS.

To configure additional Web sites:

1. In the 'Virtual Hosts' section of the 'Web server' screen, click the 'New Entry' link (see Figure 5.360). The 'Virtual Host' screen appears.

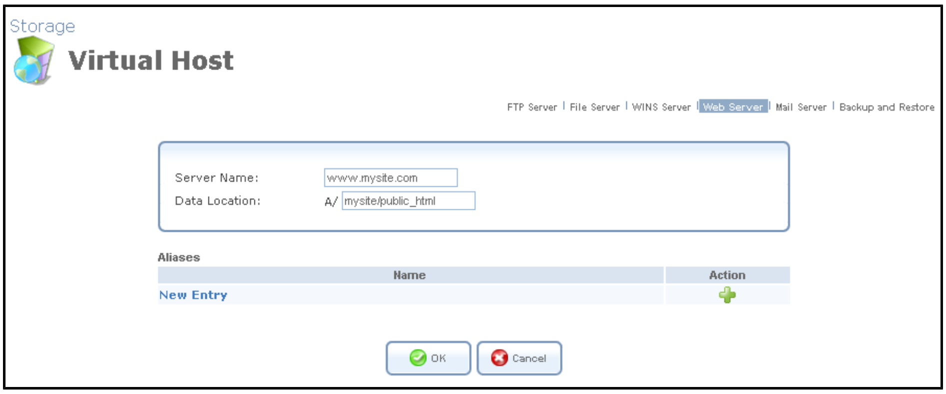


Figure 5.363 Virtual Host

2. In the 'Server Name' field, type the Web site's domain name.

3. In the 'Data Location' field, type the file system path to the OpenRG folder containing the Web site's content.

4. To add an alias to the virtual host, click the 'New Entry' link in the 'Aliases' section. The 'Virtual Host Aliases' screen appears.

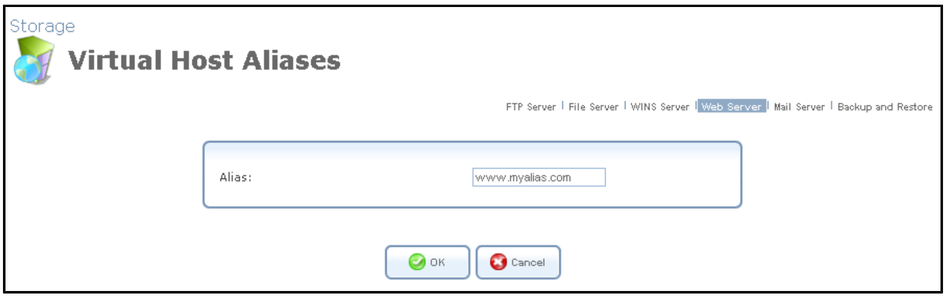


Figure 5.364 Virtual Host Aliases

5. Type an alias URL in the 'Alias' field, and click 'OK'. The new alias appears under the 'Aliases' section (see Figure 5.363).

6. Click 'OK' to save the settings. Your site's URL and alias are added to the 'Virtual Hosts' section of the Web server screen.

Virtual Hosts

Name	Aliases	Data Location	Action
www.mysite.com	www.myalias.com	mysite/public_html	
New Entry			

Figure 5.365 New Virtual Host

7. Click 'OK' to save the settings.

5.9.5 Mail Server

OpenRG can operate as a mail server, serving both users on the LAN and the WAN. Users can access their mailboxes both as a home-based service, when working within the network, or as a web-based service, when working remotely.

Note: In order for this feature to operate properly, a system storage area must be created on OpenRG's storage device. For more information, refer to Section 5.9.7.2.

5.9.5.1 Mail Server Configuration

Before configuring your mail server, you must register a domain name and map its A field (default server) or MX field (mail server) to OpenRG's WAN IP address. This can easily be done using the Dynamic DNS feature (refer to Section 5.10). To configure your mail server:

1. Access the Mail Server settings either from its link in the 'Storage' tab under the 'Services' screen, or by clicking the 'Mail Server' icon in the 'Advanced' screen. The 'Mail Server' screen appears.

Figure 5.366 Mail Server

2. Enable the mail server by checking the 'Enabled' check box. The full mail server screen appears.

Figure 5.367 Enabled Mail Server

3. Enter the registered domain name in the 'Domain' field.

4. Choose the default Inbox quota for each new mailbox in the 'Quota' section.

5. Choose the maximum number of simultaneous connections allowed to the mail server. It is recommended that this value be left at the default of three.

6. Check the Sender Policy Framework (SPF) check box to allow mail filtering (recommended).

7. Check the 'Log Messages' check box to log the senders and receivers of all the sent, received and rejected messages in the system log. It is recommended that this option remains unchecked.

8. The next three sections should be configured according to your required mail retrieval protocols. You can enable POP3, IMAP4 and IMAPS, and choose whether to allow each with WAN access, by checking the relevant check boxes.

9. Click 'OK' to save the settings.

5.9.5.2 Mailbox Configuration

To configure a mailbox:

1. Click the 'Users' icon in the 'Advanced' screen of the WBM. The 'Users' screen appears:

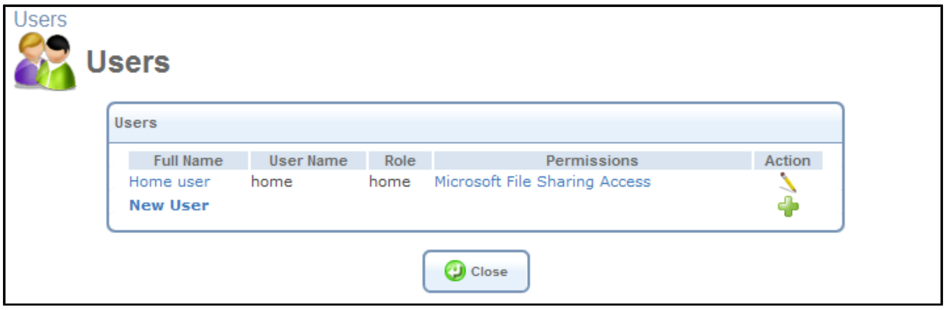


Figure 5.368 Users

2. Click the action icon of the user for which you would like to create a mailbox. The 'User Settings' screen appears:

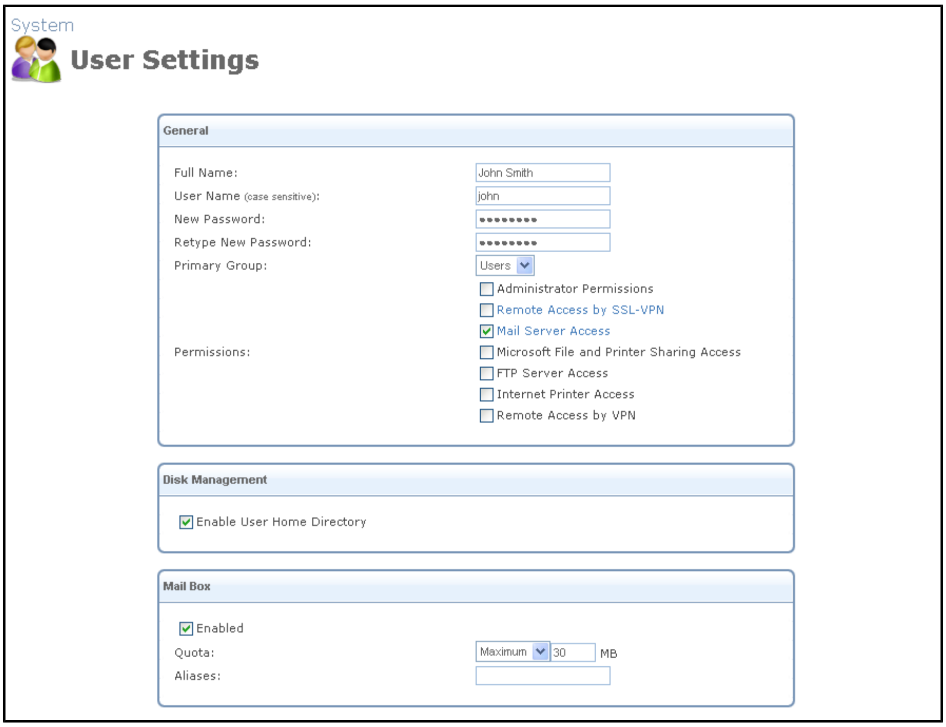


Figure 5.369 User Settings

3. In this screen, perform the following:

    1. Check the 'Enable User Home Directory' check box. This feature creates a home directory for the user.

    2. In the Permissions section, check the 'Mail Server Access' check box, to grant this permission.

    3. Enable the mailbox by checking the 'Enabled' check box in the 'Mail Box' section.

4. Click 'OK' to save the settings.

The user's email address will be <username>@<domain name> where <username> is the OpenRG username of the user, and <domain name> is the domain name configured for the mail server.

5.9.5.3 Additional Features

5.9.5.3.1 Email Aliases

You may add any number of aliases to an email address. Emails sent to an alias address will be rerouted to the main address. To configure email aliases:

1. Click the 'Users' icon in the 'Advanced' screen of the WBM. The 'Users' screen appears.

2. Click the  action icon of the user for which you would like to add aliases.

3. In the 'User Settings' screen that appears (see Figure 5.370), enter the aliases (usernames only) as a comma-separated list in the 'Aliases' field of the 'Mail Box' section.

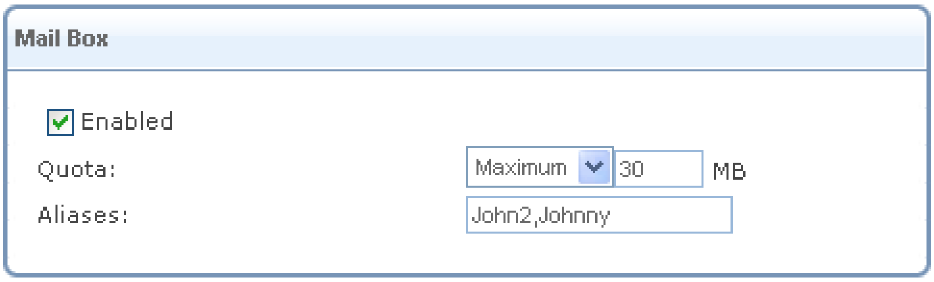


Figure 5.370 Mail Box Aliases

4. Click 'OK' to save the settings.

5.9.5.3.2 Mailing Lists

You may configure mailing lists to easily send mass emails. To configure mailing lists: Figure 5.373

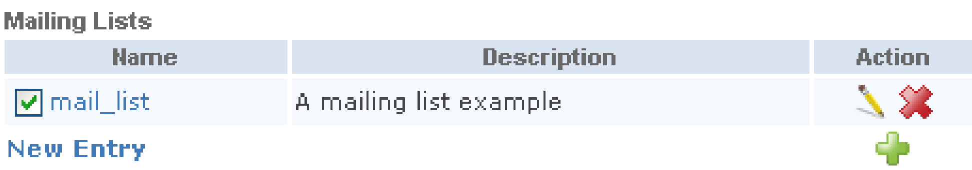


Figure 5.373 New Mailing List

1. Click the 'Mail Server' icon in the 'Advanced' screen of the WBM. The 'Mail Server' screen appears (see Figure 5.367).

2. Click the 'Mailing Lists' tab. The 'Mailing Lists' screen appears.

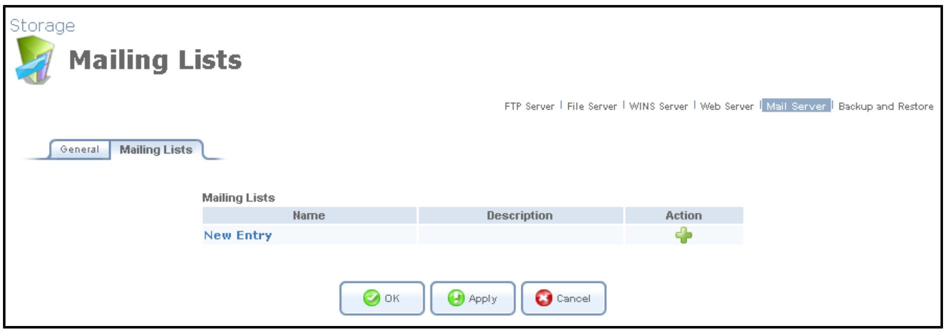


Figure 5.371 Mailing Lists

3. Click the 'New Entry' link to add a new mailing list. The 'Mailing Lists' screen appears.

Figure 5.372 Mailing Lists

4. Enter a name and description for the mailing list in their respective fields. In the 'Addresses' field, enter a comma-separated list of the email addresses that you would like to include in the mailing list. Adding local addresses requires entering the usernames only, while adding external addresses requires entering the full email addresses.

5. Click 'OK' to save the settings.

5.9.5.4 Email Client Configuration

OpenRG email clients can access their mailboxes both from within the LAN and remotely over the internet.

5.9.5.4.1 LAN Email Clients

LAN email clients should configure the following:

- The incoming and outgoing mail servers should be configured with OpenRG's LAN IP (192.168.1.1) or LAN domain name (openrg.home).

- The outgoing mail server (SMTP) does not require authentication from the LAN.

- The incoming mail server (POP3, IMAP4 or IMAPS) requires authentication of the user's username and password.

5.9.5.4.2 WAN Email Clients

WAN email clients should configure the following:

- The incoming and outgoing mail servers should be configured with OpenRG's WAN IP or WAN domain name.

- The outgoing mail server requires authentication of the user's username and password.

- The incoming mail server (POP3, IMAP4 or IMAPS) must be enabled for OpenRG's WAN, and requires authentication of the user's username and password.

5.9.6 Backup and Restore

OpenRG's backup facility allows backing up data, stored in the system storage area, to external USB disks. You may specify backups to run automatically at scheduled times. Two preliminary conditions must be met before enabling the backup mechanism:

- The file server feature must be activated and configured (refer to Section 5.9.2).
- The file server must be consisted of at least two disks.

Please note that the the backup is done at the directory level, meaning that it is not possible to backup a single stand-alone file.

5.9.6.1 Backing Up Your Data

To backup your data:

1. Access the Backup settings either from its link in the 'Advanced' tab under the 'Services' screen, or by clicking the 'Backup and Restore' icon in the 'Advanced' screen. The 'Backup and Restore' screen appears:

Figure 5.374 Backup and Restore

2. Click the 'New Entry' link in the 'Backup Schedule' section.
3. In the 'Edit Backup' screen that appears (see Figure 5.375), configure the following parameters:
   1. Type the source to backup. For example, { A/homes}.
   2. Type the destination of the backup files. For example, { B/backups}. It is recommended that the destination be an external storage device.

    3. Choose between full backup, incremental backup, or both, by scheduling a time for the backup operation. You can choose between daily, weekly or monthly backups in the 'Schedule' combo boxes.

4. Press 'OK' to save the schedule settings.

5. Press 'Backup Now' to run the backup operation immediately. When backing up, the screen will display the status and progress of the operation.

> Note: Do not schedule a monthly backup on the 31st, as backups will not run on months with 30 days.

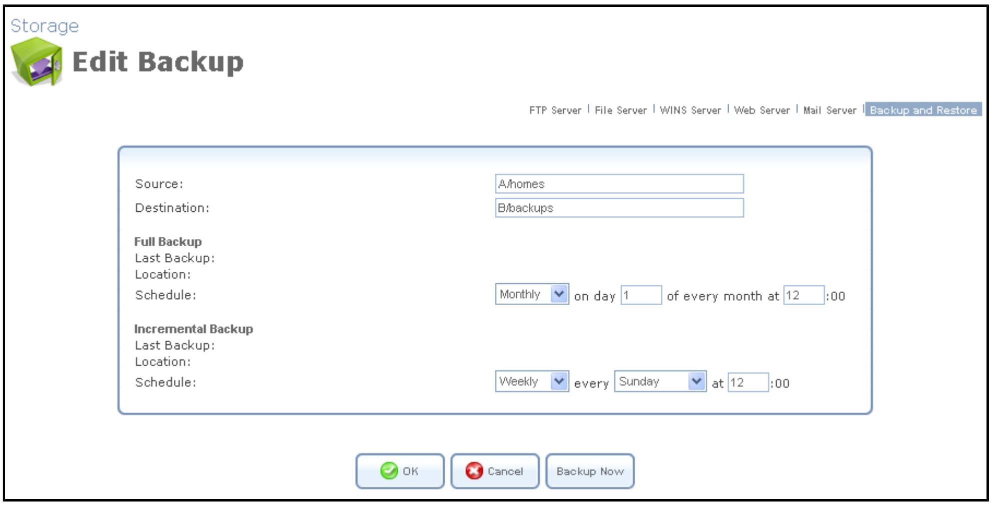


Figure 5.375 Edit Backup

5.9.6.2 Restoring Your Data

To restore your data:

1. Press the 'Backup and Restore' icon in the 'Advanced' screen of the WBM. The 'Backup and Restore' screen appears (see Figure 5.374).

2. Press the 'Restore' tab.

3. In the 'Restore' screen that appears (see Figure 5.376), configure the following parameters:

    1. Type the source to restore in the 'Source Archive' field. For example, { A/homes}.

    2. Choose whether to restore the entire archive or only a sub directory, in the 'Restore Option' combo box. If you choose sub directory, a second field appears in which you must enter the name of the sub directory, relative to the source archive. For example, to restore { A/homes/john}, type { john} as the sub directory.

    3. Choose a destination for which to restore the archive. You can choose between the original location or any other directory. If you choose the another directory, a second

field appears in which you must enter the name of the directory. Note that the path of the restored directory will be created under the path of the destination directory. For example, if you specify the directory { A/restore_dir}, the result will be { A/restore_dir/A/homes/john}.

Figure 5.376 Edit Restore

5.9.7 Managing Your Disks

The 'Storage' menu item provides access to the 'Disk Management' screen, which enables you to view and manage your storage devices.

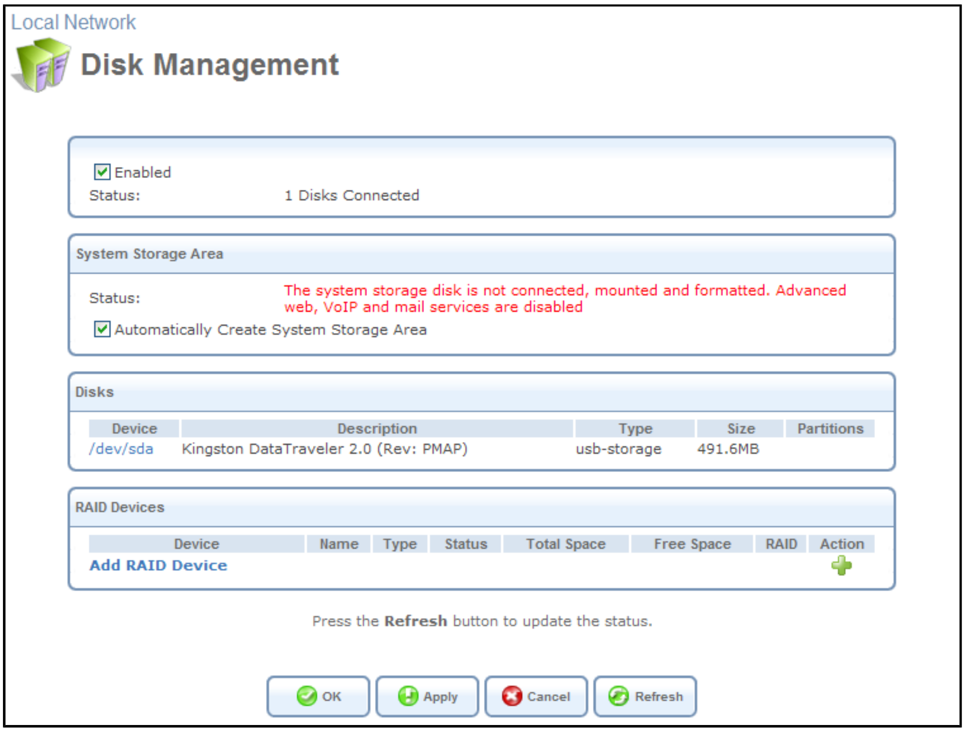


Figure 5.377 Disk Management

Enabled Select or deselect this check box to enable or disable this feature.

NetBIOS Workgroup OpenRG's workgroup name that will be displayed in the Windows network map of LAN hosts. All computers connected to OpenRG's network will appear in this workgroup.

System Storage Area OpenRG automatically defines a specific location on the storage device for storing data used by its various services. This setting is valid until the storage device is disconnected. When reconnected, OpenRG may select another partition for this purpose.

Disks This section provides details about the attached storage device. Click the name of the disk. The 'Disk Information' screen appears, providing all available information regarding the disk and its partitions.

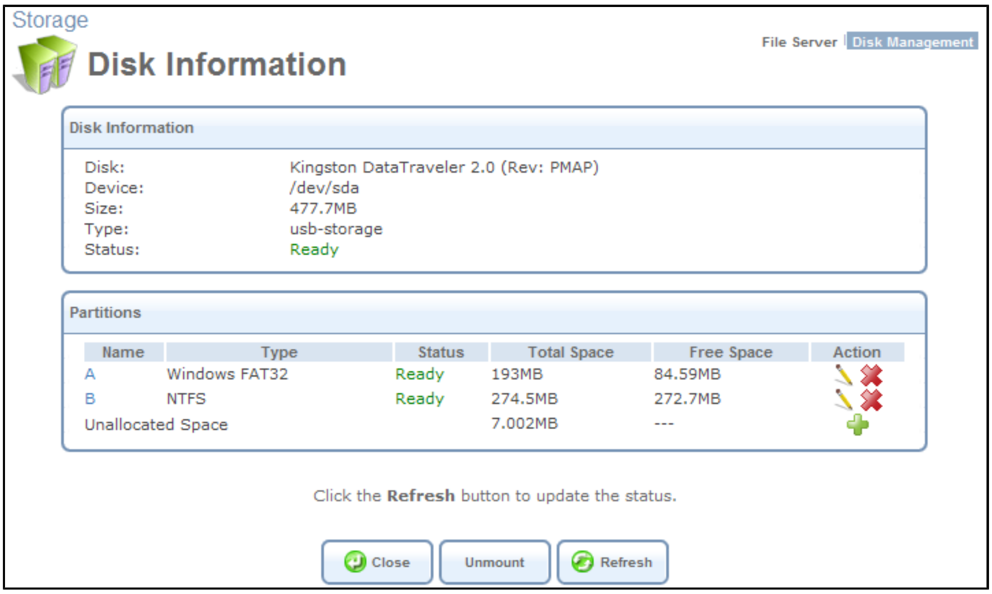


Figure 5.378 Disk Information

5.9.7.1 Managing Disk Partitions

A disk partition can be formatted, checked, or deleted. The following sections describe each of these operations.

Warning: When applying administrative changes to storage devices, services using these devices are stopped (for more information about such services, refer to Section 5.9).

5.9.7.1.1 Adding and Formatting a Partition

In order to be used, a mass storage device must first be partitioned and formatted. However, partitioning can only be performed on unallocated disk space. If your device is already partitioned, you may not be able to add a partition, unless unallocated space is available.

To add a Windows formatted partition, perform the following:

1. Click the 'Storage' menu item under the 'Services' tab. The 'Disk Management' screen appears.

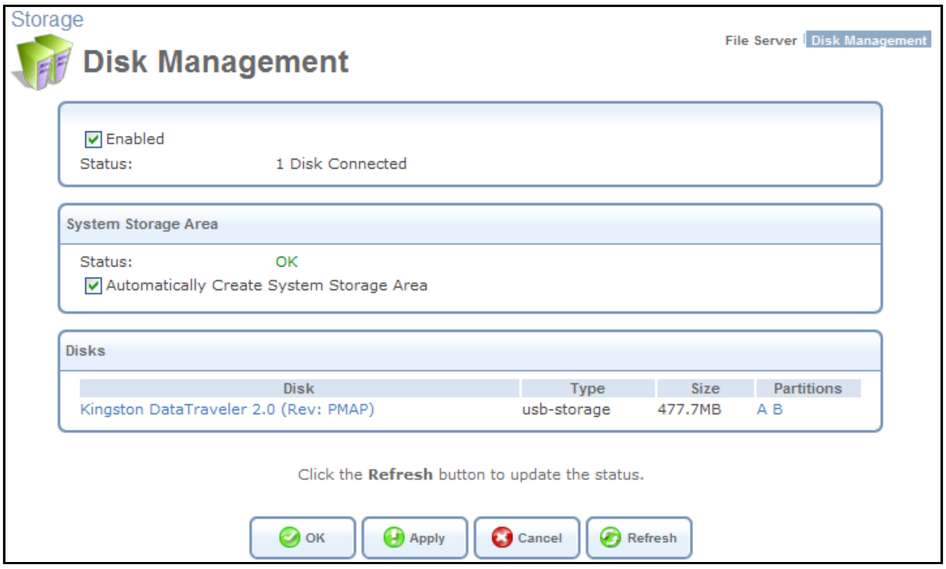


Figure 5.379 Disk Management

2. In the 'Disks' section, displaying your connected storage devices, click the disk's link. The 'Disk Information' screen appears.

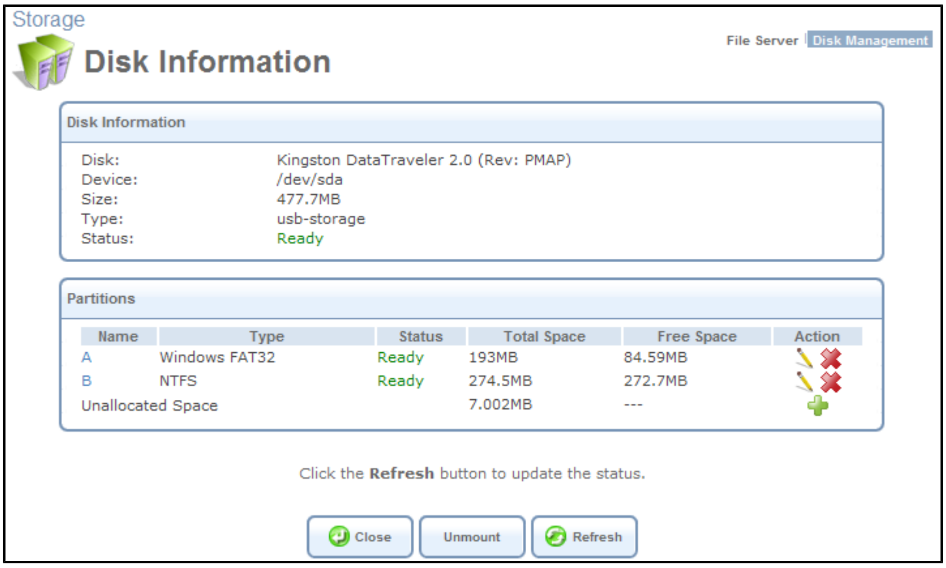


Figure 5.380 Disk Information

3. In the 'Partitions' section, click the  action icon . The 'Partition Type' screen appears.

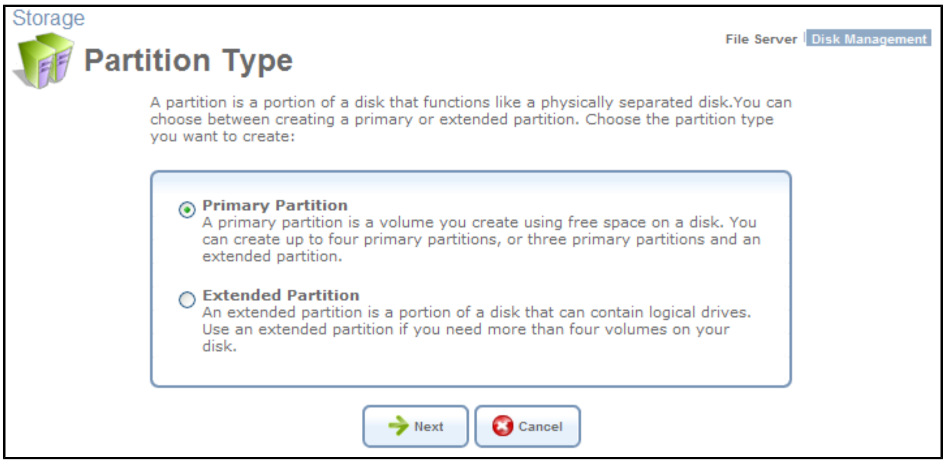


Figure 5.381 Partition Type

4. Select 'Primary Partition', and click 'Next'. The 'Partition Size' screen appears.

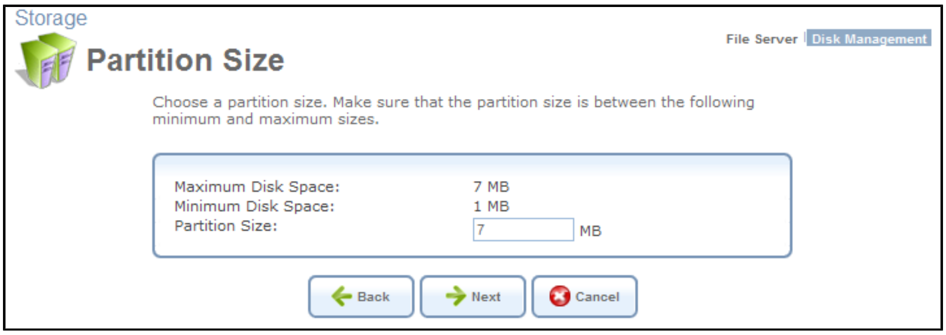


Figure 5.382 Partition Size

5. Enter a volume for the new partition (in mega bytes) and click 'Next'. The 'Partition Format' screen appears.

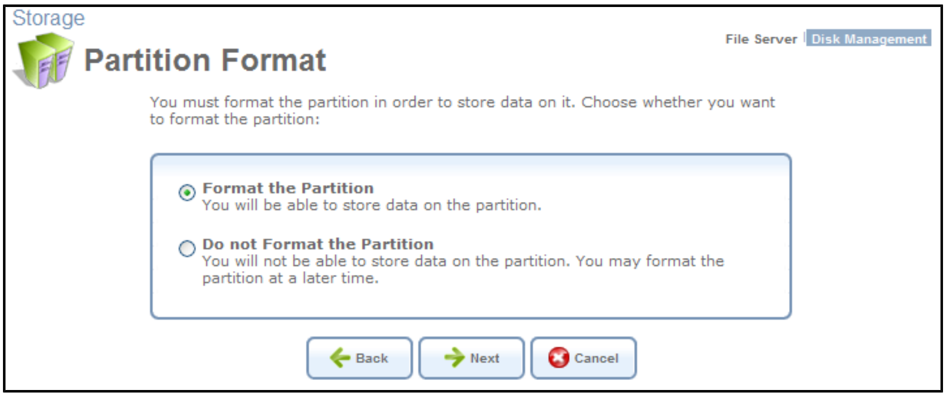


Figure 5.383 Partition Format

6. Select 'Format the Partition', and click 'Next'. The 'Partition File System' screen appears.

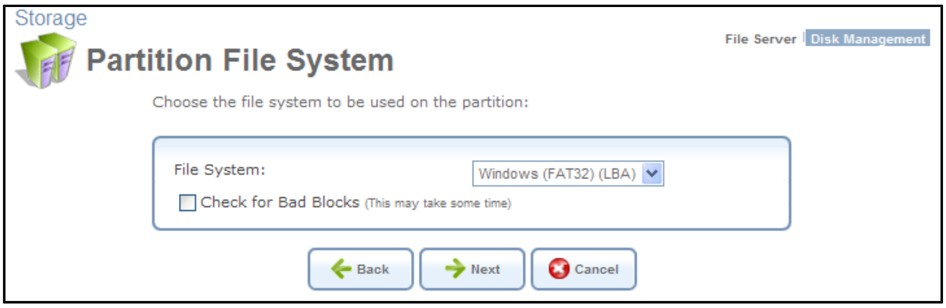


Figure 5.384 Partition File System

7. Select 'Windows (FAT32) (LBA)' as the file system for the partition and click 'Next'. The 'Partition Summary' screen appears.

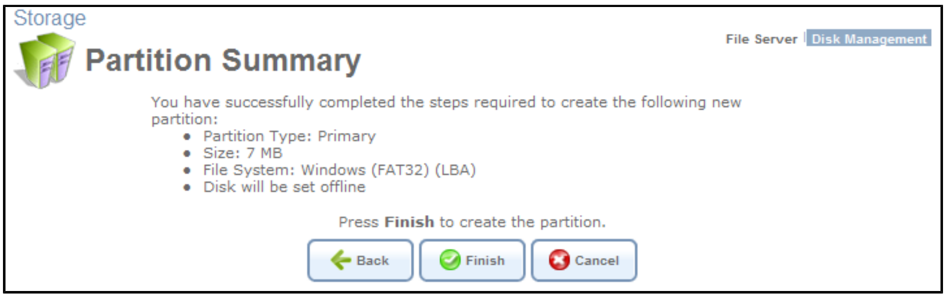


Figure 5.385 Partition Summary

8. Click 'Finish' to create the new partition. The 'Disk Information' screen reappears, refreshing as the partition formatting progresses, until the status changes to 'Ready'.

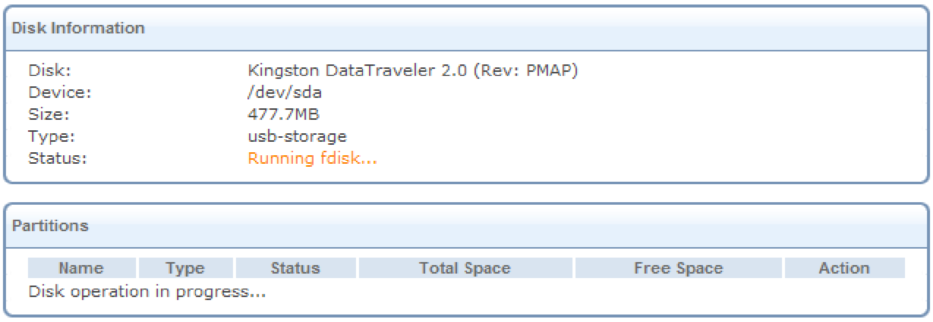


Figure 5.386 Partition Formatting in Progress

The new partition path names are designated as "A", "B", etc.

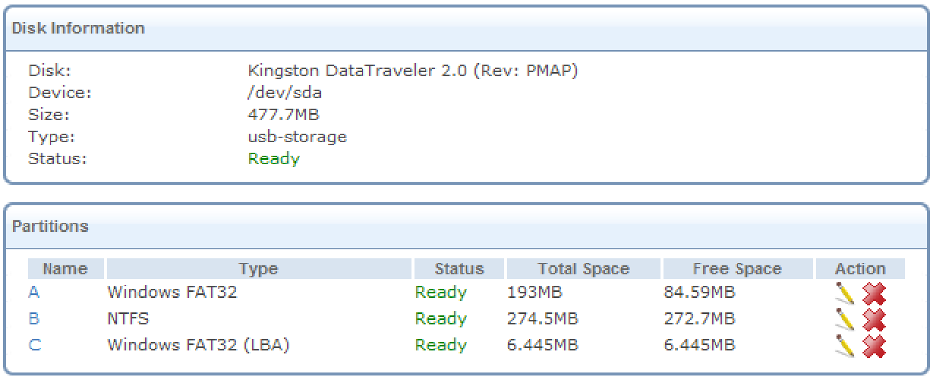


Figure 5.387 Formatting Complete – Partition Ready

To learn about additional operations you can perform on your storage device, refer to the 'Shared Storage' section of the OpenRG Administrator Manual.

5.9.7.1.2 Checking a Partition

Periodically, you should check the disk's partitions for the presence of bad sectors, to maintain the disk's health and prevent data loss.

To check a partition:

1. In the 'Disks' section of the 'Disk Management' screen, click the disk's link. The 'Disk Information' screen appears.

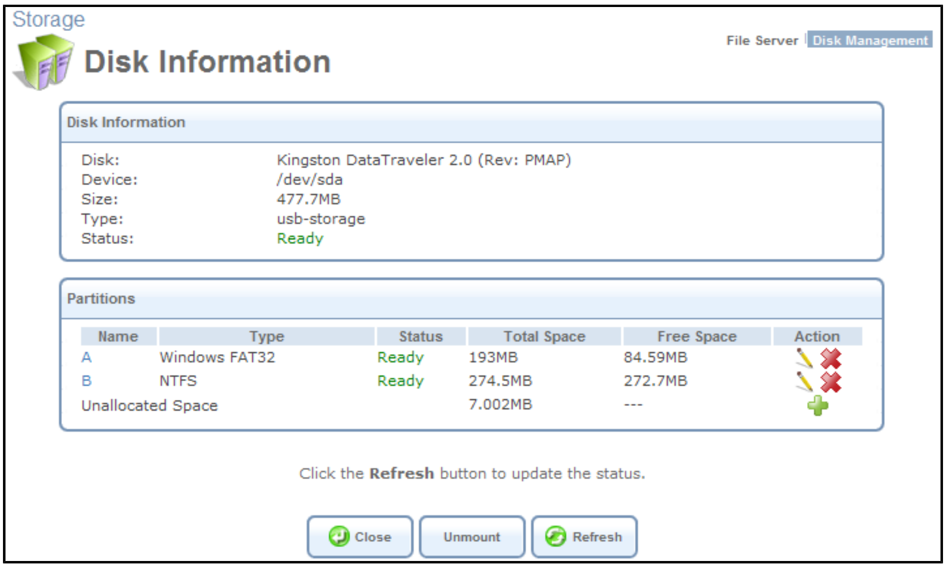


Figure 5.388 Disk Information

2. In the 'Partitions' section, click the  action icon of the partition you would like to check. The 'Partition Properties' screen appears.

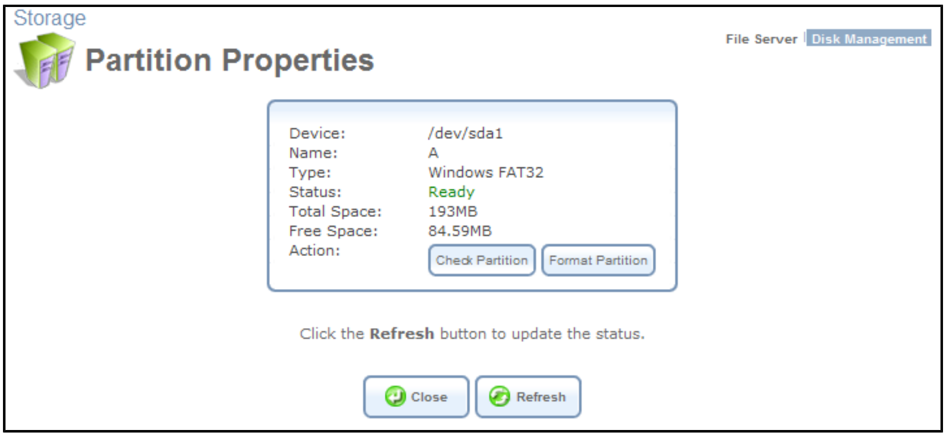


Figure 5.389 Partition Properties

3. Click the 'Check Partition' button. The 'Partition Check' screen appears.

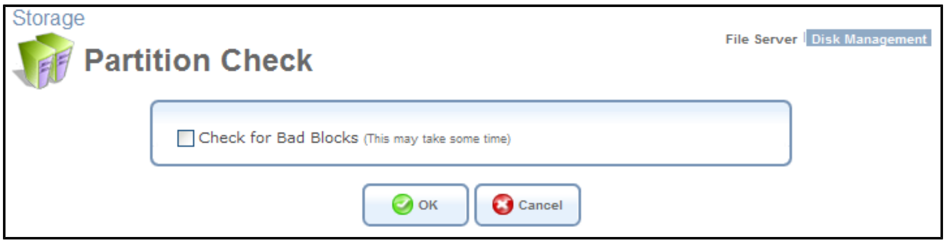


Figure 5.390 Partition Check

This screen enables you to check a partition for presence of bad blocks prior to the regular file system checkup. To do so, select the 'Check for Bad Blocks' check box.

4. Click 'Next'. A warning screen appears, alerting you that the partition will be set to offline.

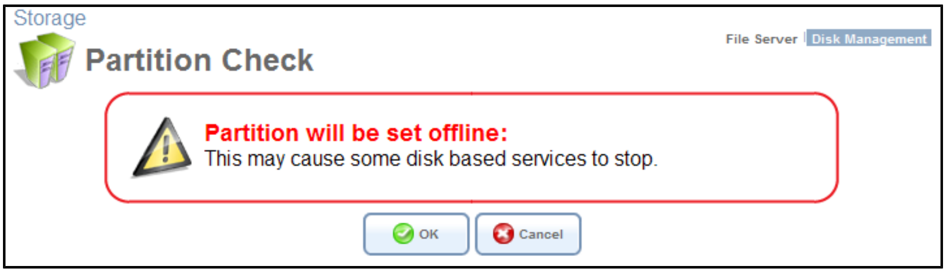


Figure 5.391 Offline Partition Warning

5. Click 'OK' to check the partition. The screen refreshes as the partition checking progresses.

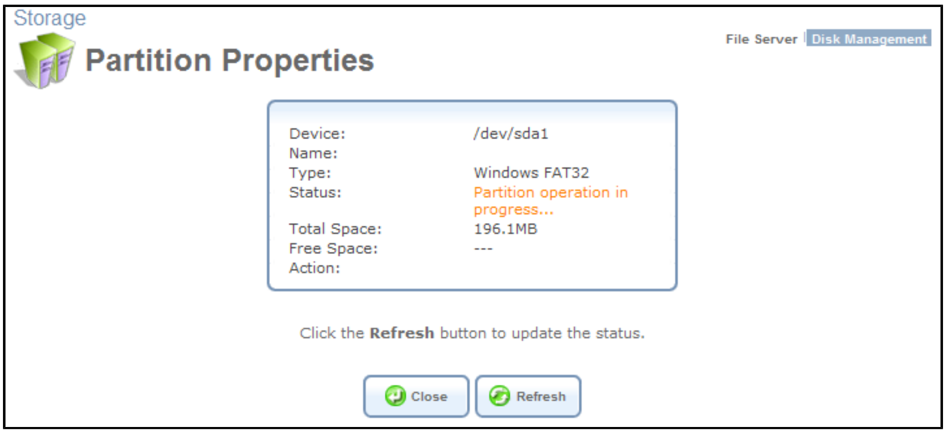


Figure 5.392 Partition Checking in Progress

When the check is complete, the status changes to 'Ready'.

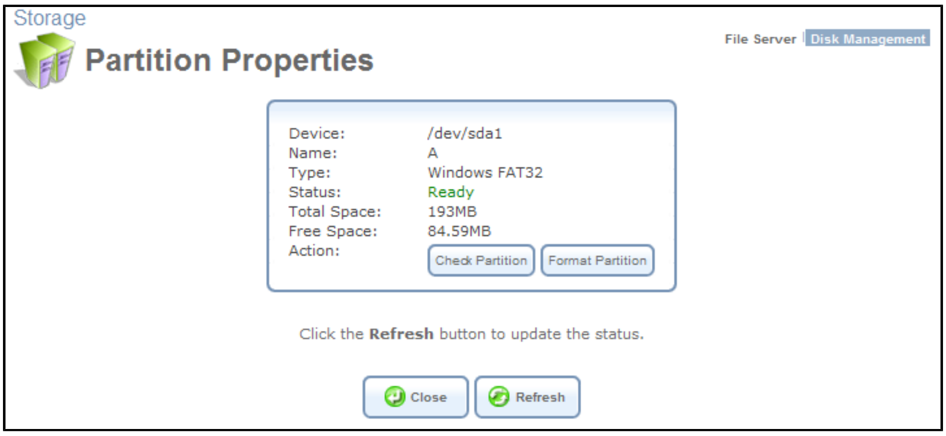


Figure 5.393 Checking Complete – Partition Ready

5.9.7.1.3 Reformatting a Partition

In addition to formatting a newly created partition, you can reformat an existing partition with either EXT2, EXT3, or FAT32 file systems. Unless your gateway is based on the Intel IXP425 or Infineon platform, a partition can also be formatted with NTFS, allowing both *Read* and *Write* access. OpenRG running on the Intel IXP425 or Infineon platforms identifies a storage device formatted with NTFS, but only allows *Read* access to it.

Note: For security reasons, it is recommended to format disk partitions with the EXT2 or EXT3 file system.

To reformat a partition:

1. In the 'Disks' section of the 'Disk Management' screen, click the disk's link. The 'Disk Information' screen appears.

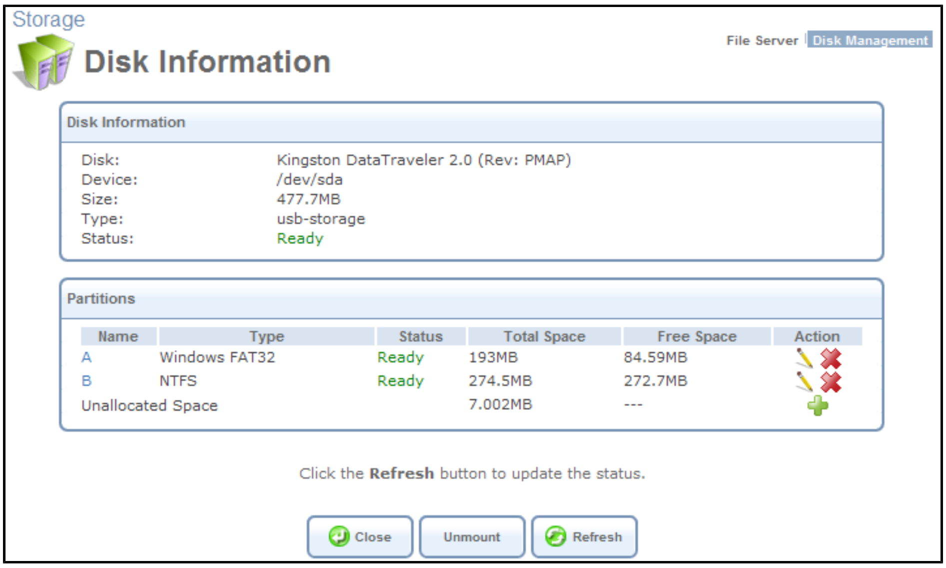


Figure 5.394 Disk Information

2. In the 'Partitions' section, click the  action icon of the partition you would like to edit. The 'Partition Properties' screen appears.

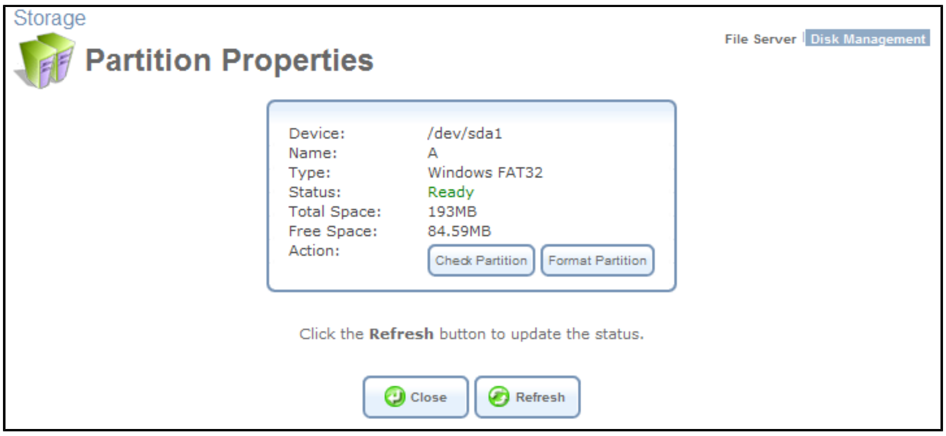


Figure 5.395 Partition Properties

3. Click the 'Format Partition' button. The 'Partition Format' screen appears.

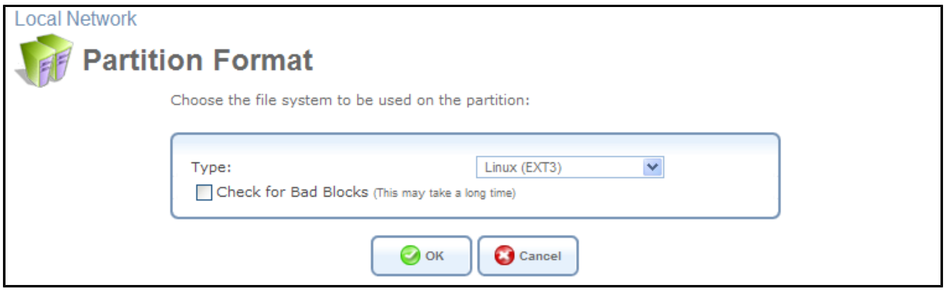


Figure 5.396 Partition Format

Note: You can also instruct OpenRG to check the disk for bad blocks prior to formatting it, by selecting the corresponding check box. Only the disk space consisting of healthy blocks will be formatted. Bad blocks will be ignored.

4. Select a file system for the partition and click 'Next'. A warning screen appears, alerting you that all the data on the partition will be lost.

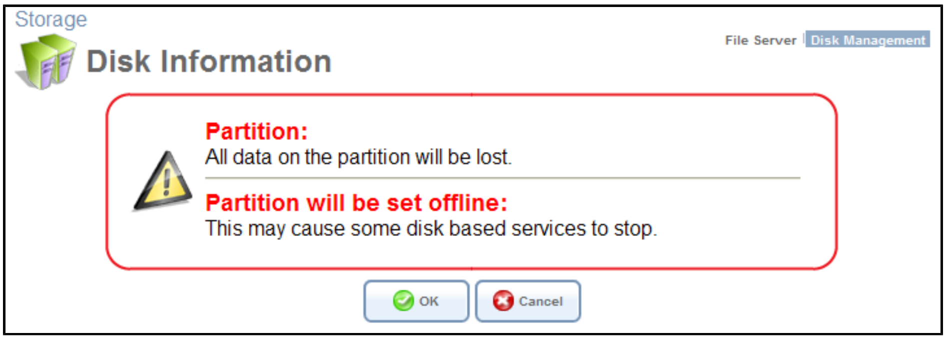


Figure 5.397 Lost Data Warning

5. Click 'OK' to format the partition. The screen refreshes as the partition formatting progresses.

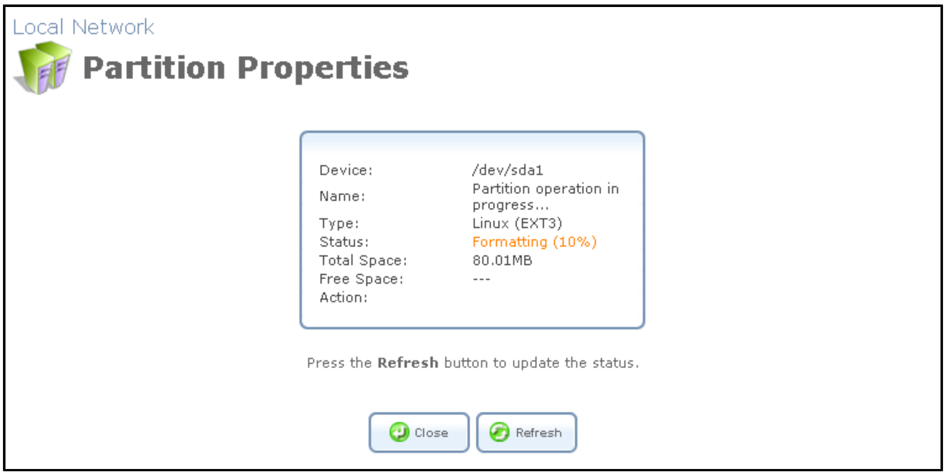


Figure 5.398 Partition Formatting in Progress

When the format is complete, the status changes to 'Ready'.

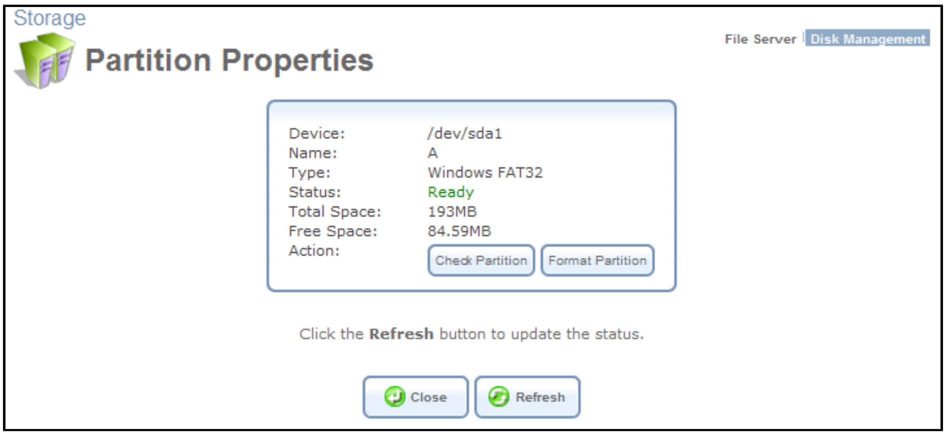


Figure 5.399 Formatting Complete – Partition Ready

5.9.7.1.4 Deleting a Partition

If you would like to delete a partition on your storage device, perform the following:

1. In the 'Disks' section of the 'Disk Management' screen, click the disk's link. The 'Disk Information' screen appears.

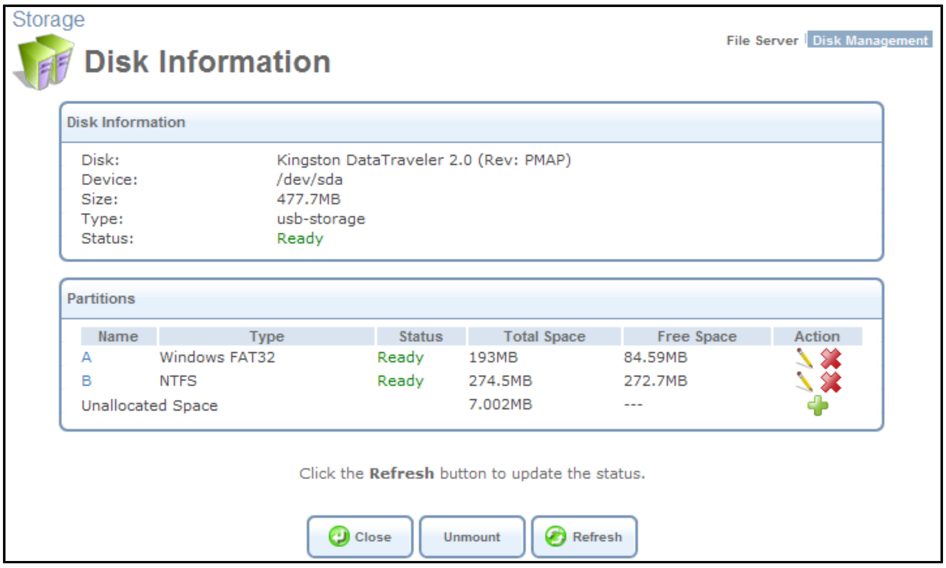


Figure 5.400 Disk Information

2. In the 'Partitions' section, click the  action icon of the partition you would like to delete. A warning screen appears, alerting you that all the data on the partition will be lost.

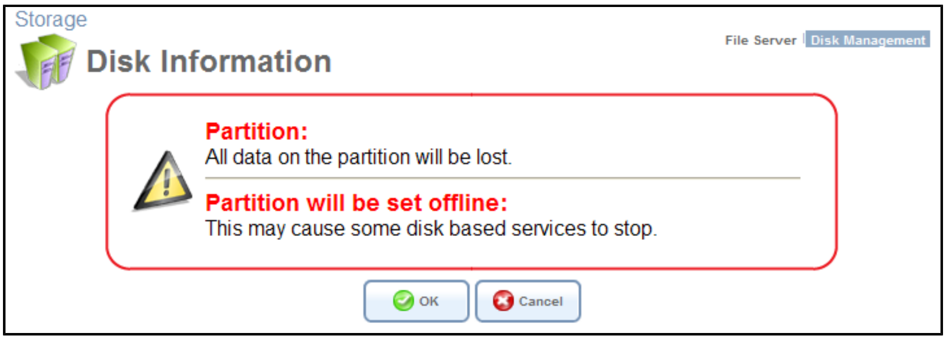


Figure 5.401 Lost Data Warning

3. Click 'OK' to delete the partition.

5.9.7.2 Changing the System Storage Area Location

OpenRG uses a specific location on a storage device for storing data used by its various services. The following services use the system storage area:

- Printer spool and drivers
- Mail server spool
- Backup of OpenRG's configuration file (rg_conf)
- PBX-related audio files for voice mail, auto attendants and music on-hold
- FTP server
- Mail boxes information
- Users' home directories
- Web server content

If you would like to set a specific partition as the location for the system storage area, perform the following:

1. Deselect the 'Automatically Create System Storage Area' check box. The screen refreshes displaying the 'System Storage Area' field (containig the auto-selected partition).

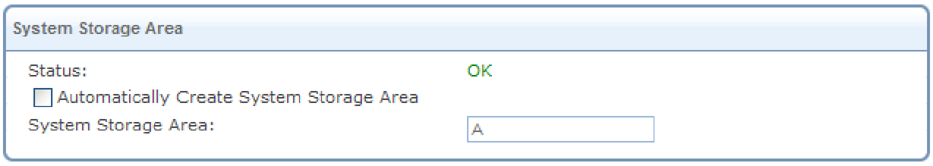


Figure 5.402 Manually Defined System Storage Area

2. Enter the letter of the partition to which you would like to set the system storage area.

3. Click 'OK' to save the settings.

If you wish to view the system directories, verify that the system storage area is shared (refer to Section 5.9.2.1). Then, browse to `\\openrgdrive\<PARTITION LETTER>` (use Windows Explorer if you are using a browser other than Internet Explorer).

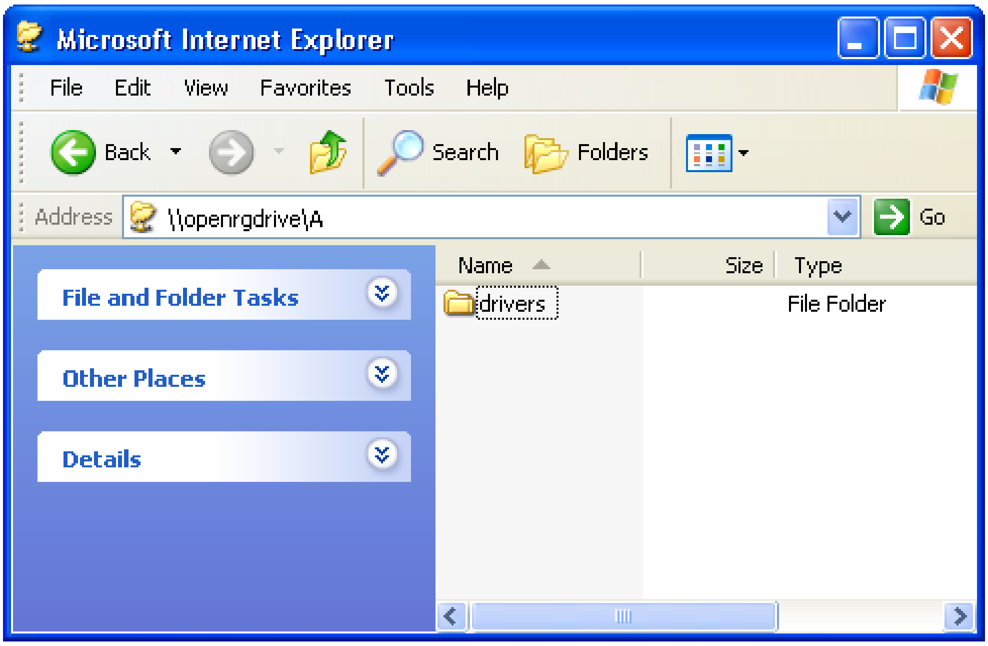


Figure 5.403 System Storage Area Directories

> Note: Data cannot be written to partitions formatted with NTFS, unless OpenRG is based on the Conexant Solos, Mindspeed Malindi2 or Freescale platform. Consequently, if you define an NTFS partition as the system storage area, the services mentioned earlier will not operate on OpenRG, displaying a warning message.

5.10 Accessing Your Network Using a Domain Name

OpenRG's Dynamic DNS (DDNS) service enables you to define a unique domain name for your gateway's Internet connection, thereby allowing you to access the gateway or your home network's services just by pointing the browser to this name. When using this feature, you will not need to check and remember your gateway's Internet IP address, which may change in case of a disconnection from the ISP's network.

5.10.1 Opening a Dynamic DNS Account

In order to use the DDNS feature, you must first obtain a DDNS account. OpenRG provides a list of DDNS servers on which you may create such an account. To view this list, perform the following:

1. Access this feature either from the 'Advanced' tab under the 'Services' screen, or by clicking its icon in the 'Advanced' screen. The 'Dynamic DNS' connections screen appears.

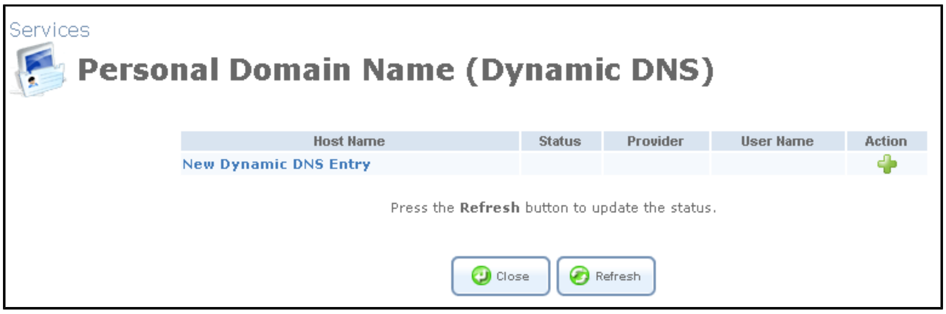


Figure 5.404 Personal Domain Name (Dynamic DNS)

2. Click the 'New Dynamic DNS Entry' link to add a new DDNS entry. The following screen appears.

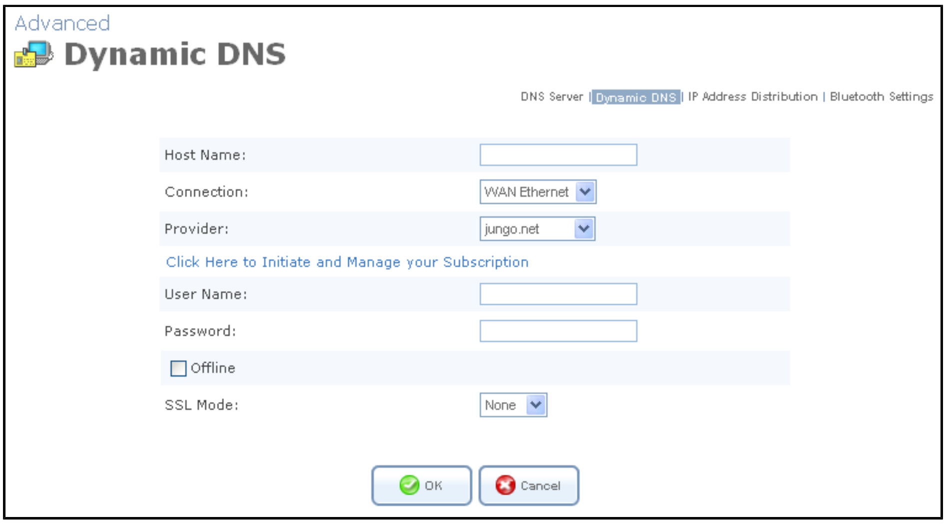


Figure 5.405 Dynamic DNS Entry

3. Specify the DDNS parameters:

Host Name Enter your full DDNS domain name.

Connection You can couple the DDNS service with your WAN Ethernet connection. The DDNS service will only use the chosen device, unless *failover* is enabled. In this case, the failed-to device will be used instead (assuming its route rules consent), until the chosen device is up again. For more information on failover, refer to Section 6.6.1.3.3.

Provider Select your DDNS service provider. The screen will refresh, displaying the parameters required by each provider. The provider depicted herein is `dyndns.org`, which includes all available parameters.

Click Here to Initiate and Manage your Subscription Clicking this link will open the selected provider's account creation Web page. For example, when `dyndns.org` is selected, the following page will open: http://www.dyndns.com/account/.

User Name Enter your DDNS user name.

Password Enter your DDNS password.

Wildcard Select this check-box to enable use of special links such as http://www.<your host>.dyndns.com.

Mail Exchanger Enter your mail exchange server address, to redirect all e-mails arriving at your DDNS address to your mail server.

Backup MX Select this check box to designate the mail exchange server to be a backup server.

Offline If you wish to temporarily take your site offline (prevent traffic from reaching your DDNS domain name), select this check box to enable redirection of DNS requests to an alternative URL, predefined in your DDNS account. The availability of this feature depends on your account's level and type of service.

SSL Mode With OpenRG versions that support Secure Socket Layer (SSL), secured DDNS services are accessed using HTTPS. Upon connection, OpenRG validates the DDNS server's certificate. Use this entry to choose the certificate's validation method.

None Do not validate the server's certificate.

Chain Validate the entire certificate chain. When selecting this option, the screen will refresh (see Figure 5.406), displaying an additional drop-down menu for selecting whether to validate the certificate's expiration time. Choose 'Ignore' or 'Check' respectively. If the certificate has expired, the connection will terminate immediately.

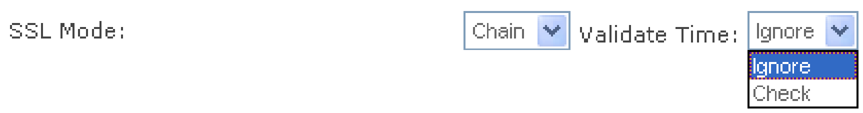


Figure 5.406 SSL Mode

Direct Ensure that the server's certificate is directly signed by the root certificate. This option also provides the 'Validate Time' drop-down menu for validation of the certificate's expiration time, as described above.

5.11 Configuring Your Gateway's IP Address Distribution

Your gateway's Dynamic Host Configuration Protocol (DHCP) server makes it possible to easily add computers that are configured as DHCP clients to the home network. It provides a mechanism for allocating IP addresses and delivering network configuration parameters to such hosts. OpenRG's default DHCP server is the LAN bridge. A client (host) sends out a broadcast message on the LAN requesting an IP address for itself. The DHCP server then checks its list

of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as `taken'. At this point the host is configured with an IP address for the duration of the lease.

The host can choose to renew an expiring lease or let it expire. If it chooses to renew a lease then it will also receive current information about network services, as it did with the original lease, allowing it to update its network configurations to reflect any changes that may have occurred since it first connected to the network. If the host wishes to terminate a lease before its expiration it can send a release message to the DHCP server, which will then make the IP address available for use by others.
Your gateway's DHCP server:

- Displays a list of all DHCP host devices connected to OpenRG
- Defines the range of IP addresses that can be allocated in the LAN
- Defines the length of time for which dynamic IP addresses are allocated
- Provides the above configurations for each LAN device and can be configured and enabled/ disabled separately for each LAN device
- Enables you to assign a static IP lease to a LAN computer, so that the computer will receive the same IP address each time it connects to the network, even if this IP address is within the range of addresses that the DHCP server may assign to other computers
- Provides the DNS server with the host name and IP address of each computer that is connected to the LAN

5.11.1 Viewing and Configuring the DHCP Settings

To view the DHCP server's settings,either use its link in the 'Advanced' tab under the 'Services' screen, or click the 'IP Address Distribution' icon in the 'Advanced' screen. The 'IP Address Distribution' screen appears, displaying the available network interfaces and their DHCP settings.

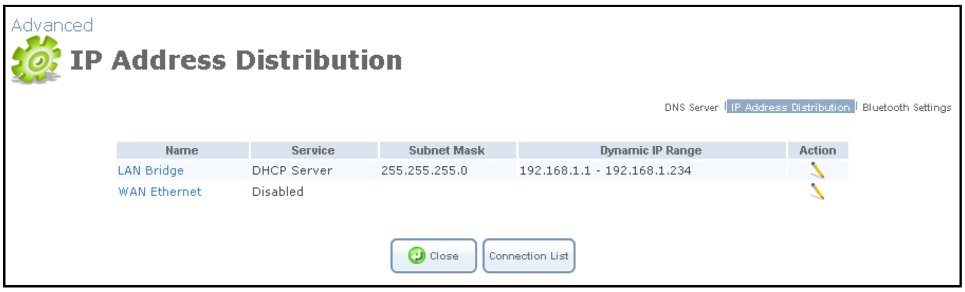


Figure 5.407 IP Address Distribution

To edit the DHCP server settings for a device:

1. Click the device's action icon . The DHCP settings screen for this device appears.

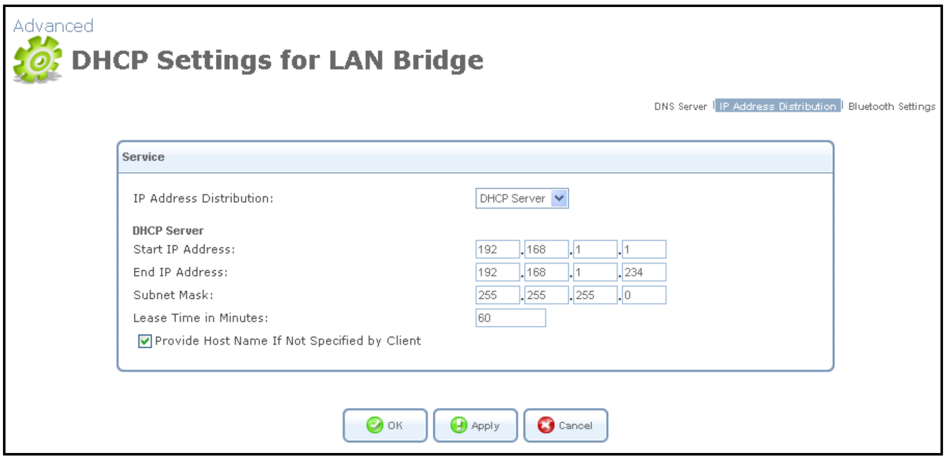


Figure 5.408 DHCP Settings for LAN Bridge

2. Select the DHCP service:

   Disabled Disable the DHCP server for this device.

   DHCP Server Enable the DHCP server for this device.

3. In case you have chosen DHCP Server, complete the following fields:

   Start IP Address The first IP address that may be assigned to a LAN host. Since the LAN interface's default IP address is 192.168.1.1, it is recommended that the first address assigned to a LAN host will be 192.168.1.2 or greater.

   End IP Address The last IP address in the range that can be used to automatically assign IP addresses to LAN hosts.

   Subnet Mask A mask used to determine to what subnet an IP address belongs. An example of a subnet mask value is 255.255.255.0.

   Lease Time In Minutes Each device will be assigned an IP address by the DHCP server for this amount of time, when it connects to the network. When the lease expires the server will determine if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use will become available for other computers on the network.

   Provide Host Name If Not Specified by Client If the DHCP client does not have a host name, the gateway will automatically assign one for it.

4. Click 'OK' to save the settings.

5.11.2 DHCP Connections

To view a list of computers currently recognized by the DHCP server, click the 'Connection List' button that appears at the bottom of the 'IP Address Distribution' screen (see Figure 5.407). The 'DHCP Connections' screen appears.

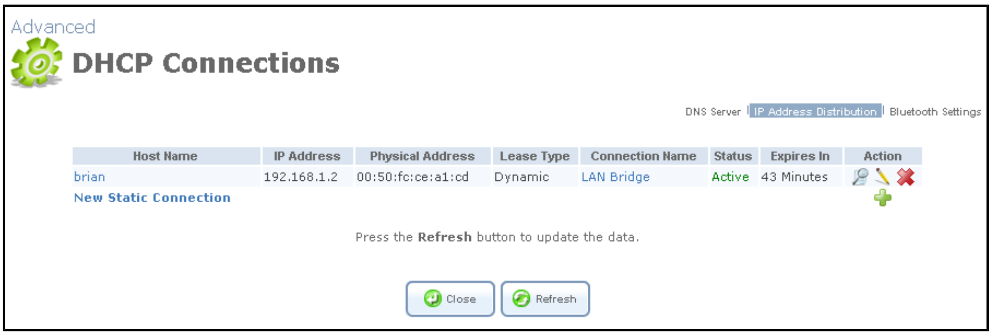


Figure 5.409 DHCP Connections

To define a new connection with a fixed IP address:

1. Click the 'New Static Connection' link. The 'DHCP Connection Settings' screen appears:

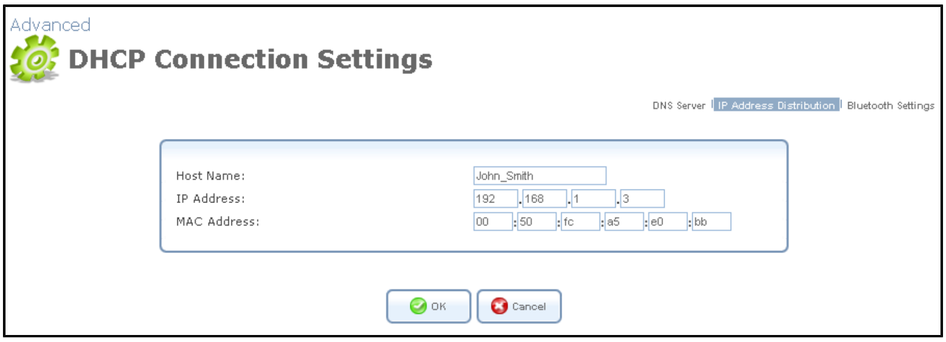


Figure 5.410 DHCP Connection Settings

2. Enter a host name for this connection.
3. Enter the fixed IP address that you would like to have assigned to the computer.
4. Enter the MAC address of the computer's network card.

> Note: A device's fixed IP address is actually assigned to the specific network card's (NIC) MAC address installed on the LAN computer. If you replace this network card then you must update the device's entry in the DHCP Connections list with the new network card's MAC address.

5. Click 'OK' to save the settings.

The 'DHCP Connections' screen will reappear (see Figure 5.411), displaying the defined static connection. This connection can be edited or deleted using the standard action icons.

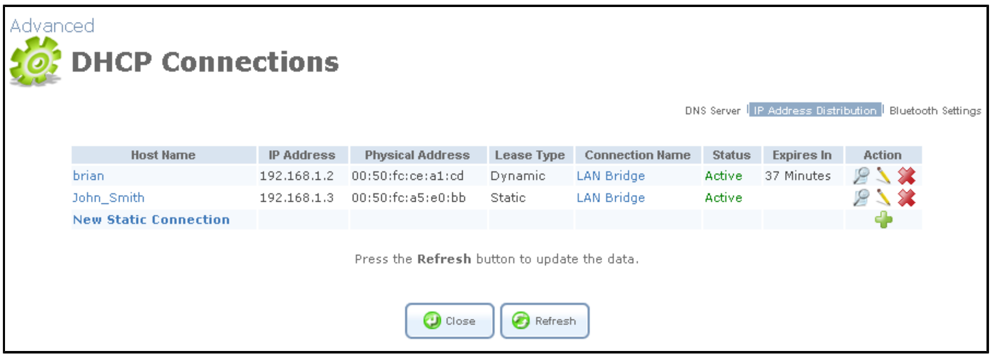


Figure 5.411 DHCP Connections

5.12 Advanced

5.12.1 DNS Server

Domain Name System (DNS) provides a service that translates domain names into IP addresses and vice versa. The gateway's DNS server is an auto-learning DNS, which means that when a new computer is connected to the network the DNS server learns its name and automatically adds it to the DNS table. Other network users may immediately communicate with this computer using either its name or its IP address. In addition your gateway's DNS:

- Shares a common database of domain names and IP addresses with the DHCP server.
- Supports multiple subnets within the LAN simultaneously.
- Automatically appends a domain name to unqualified names.
- Allows new domain names to be added to the database using OpenRG's WBM.
- Permits a computer to have multiple host names.
- Permits a host name to have multiple IPs (needed if a host has multiple network cards).

The DNS server does not require configuration. However, you may wish to view the list of computers known by the DNS, edit the host name or IP address of a computer on the list, or manually add a new computer to the list.

5.12.1.1 Viewing and Modifying the DNS Table

- To view the list of computers stored in the DNS table:

  1. Access this feature either from the 'Advanced' tab under the 'Services' screen, or by clicking its icon in the 'Advanced' screen. The DNS table will be displayed (see Figure 5.412).

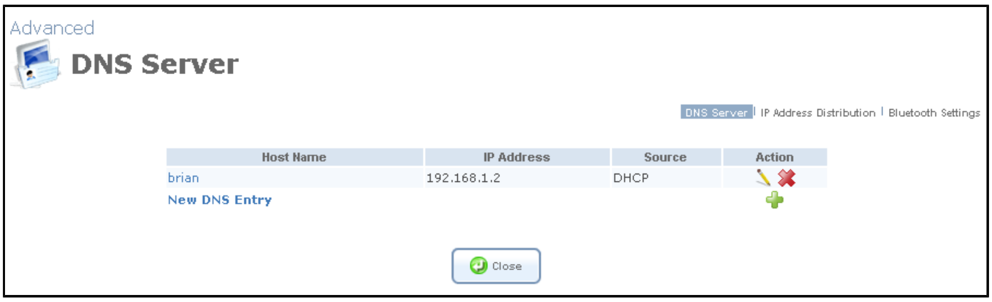


Figure 5.412 DNS Table

- To add a new entry to the list:

  1. Click the 'New DNS Entry' button. The 'DNS Entry' screen will appear (see Figure 5.413).
  2. Enter the computer's host name and IP address.
  3. Click 'OK' to save the settings.

Figure 5.413 Add or Edit a DNS Entry

- To edit the host name or IP address of an entry:

  1. Click the 'Edit' button that appears in the Action column. The 'DNS Entry' screen appears (see Figure 5.413).
  2. If the host was manually added to the DNS Table then you may modify its host name and/or IP address, otherwise you may only modify its host name.
  3. Click 'OK' to save the settings.

- To remove a host from the DNS table:

  1. Click the 'Delete' button that appears in the Action column. The entry will be removed from the table.

5.12.2 Bluetooth Settings

Yet another method to connect to OpenRG's LAN is by Bluetooth, an open specification for wireless, short-range transmission between PCs, mobile phones and other portable devices. When connected to OpenRG via Bluetooth, users can benefit from standard network connectivity, limited only by the capabilities of their connected devices. OpenRG utilizes the Bluetooth Network Encapsulation Protocol (BNEP), used by the Bluetooth Personal Area Network (PAN) profile. This layer encapsulates packets from various networking protocols, which are transported directly over the Logical Link Control and Adaptation Protocol (L2CAP) layer.

> Hardware Note: Platforms that do not feature an integrated Bluetooth chip, require a Linux-supported Bluetooth dongle, which can be connected to the gateway either by USB or PCI.

As soon as a Bluetooth dongle is connected, OpenRG can be found and connected to by Bluetooth devices. To configure OpenRG's Bluetooth settings, perform the following steps:

1. Access the Bluetooth settings either from its link in the 'Advanced' tab under the 'Services' screen, or by clicking the 'Bluetooth Settings' icon in the 'Advanced' screen. The 'Bluetooth Settings' screen appears. Select the 'Enabled' check box to enable this feature.

Figure 5.414 Bluetooth Settings

Enabled Select this check-box to enable Bluetooth connections to OpenRG.

Host Name OpenRG's identification name in the PAN. You can change the default to any string.

Authentication Level Select the level of authentication to be performed upon a connection request:

None Connect without authentication.

Enabled Enable authentication using a pin number, which will have to be provided by the device wishing to connect.

Encrypt Enable and encrypt the authentication method.

PIN Enter a value for the authentication/encryption key if you selected the 'Enabled' or 'Encrypted' options above.

2. Click 'OK' to save the settings.

The new Bluetooth connection will be added to the network connections list under the LAN bridge, and will be configurable like any other connection.

5.12.3 RADIUS Server

A Remote Authentication Dial-in User Service (RADIUS) server is most commonly a "third party" server, used for authentication of wireless clients who wish to connect to an access point. The wireless client contacts an access point (a RADIUS client), which in turn communicates with the RADIUS server. The RADIUS server performs the authentication by verifying the client's credentials, to determine whether the device is authorized to connect to the access point's LAN. If the RADIUS server accepts the client, it responds by exchanging data with the access point, including security keys for subsequent encrypted sessions. OpenRG can act both as a RADIUS client and a server, and can be used for the authentication of any clients—wireless or wired.
This enables a scenario of multiple gateways acting as RADIUS clients, connected to a "master" gateway that acts as a RADIUS server. Such a scenario can be useful in an enterprise consisting of multiple divisions.

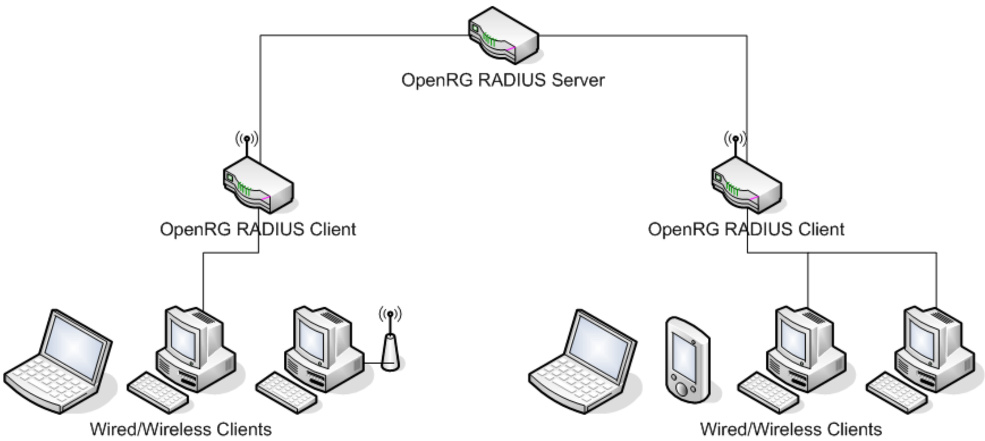


Figure 5.415 RADIUS Server Scenario

5.12.3.1 RADIUS Server Configuration

OpenRG as a RADIUS client is described in the LAN Wireless section of this manual (section Section 6.4.6). To configure OpenRG as a RADIUS server, perform the following:

1. Access the RADIUS Server settings either from the link in the 'Advanced' tab under the 'Services' screen, or by clicking the 'RADIUS Server' icon in the 'Advanced' screen. The 'RADIUS Server' screen appears.

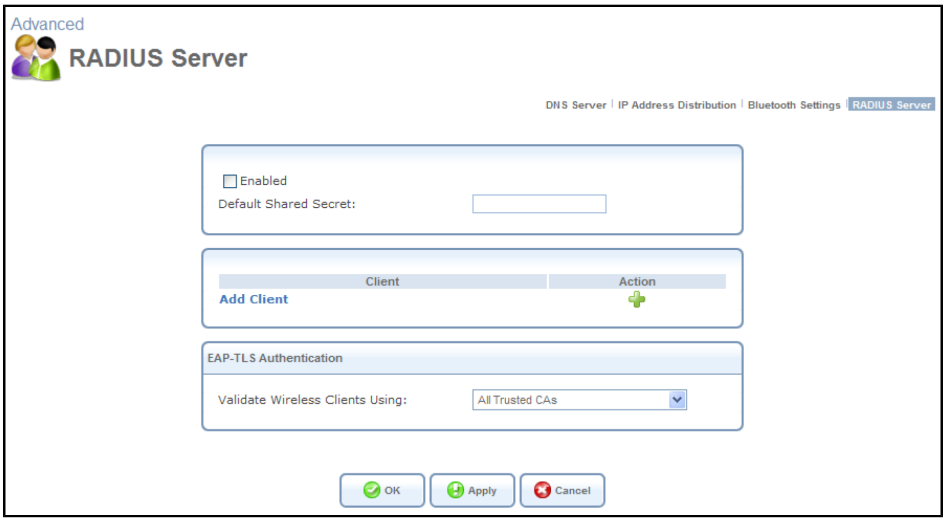


Figure 5.416 RADIUS Server

2. Check the 'Enabled' check box to enable this feature.

3. If you would like to set a shared secret that any RADIUS client can provide when requesting authentication, specify a 'Default Shared Secret'.

4. You can also set specific shared secrets for known clients by clicking 'Add Client'. The 'Add RADIUS Client' screen appears.

Figure 5.417 Add RADIUS Client

5. Enter the client's IP address and a shared secret value, and click 'OK'. You are routed back to the 'RADIUS Server' screen, which now displays the newly added client.

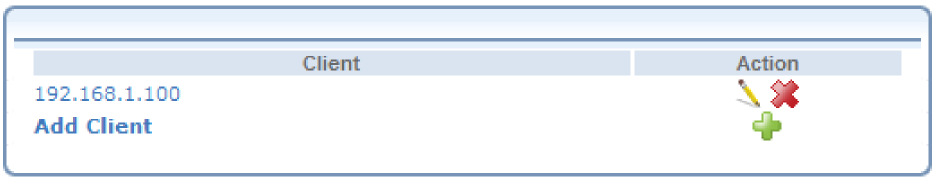


Figure 5.418 Newly Added Client

5.12.3.2 RADIUS Authentication Algorithms

OpenRG's RADIUS server utility uses six different authentication algorithms. These are:

- PAP
- CHAP
- MSCHAP
- MSCHAP v2
- EAP PEAP MSCHAP v2
- EAP TLS

While the first four use only username and password combinations for authentication, the EAP-PEAP algorithm utilizes the server's certificate for authentication, and EAP TLS authenticates both the client and server with certificates (for more information about certificates, refer to Section 6.9.4). When a request is received from a client, a negotiation begins in which certificates are passed between the client and server, resolving in either acceptance or rejection. In the 'EAP-TLS Authentication' section of the 'RADIUS Server' screen, you can select the certificate by which to validate wireless clients. Select "All Trusted CAs" to validate a client with any of OpenRG's trusted certificates, or choose a specific certificate from the list.

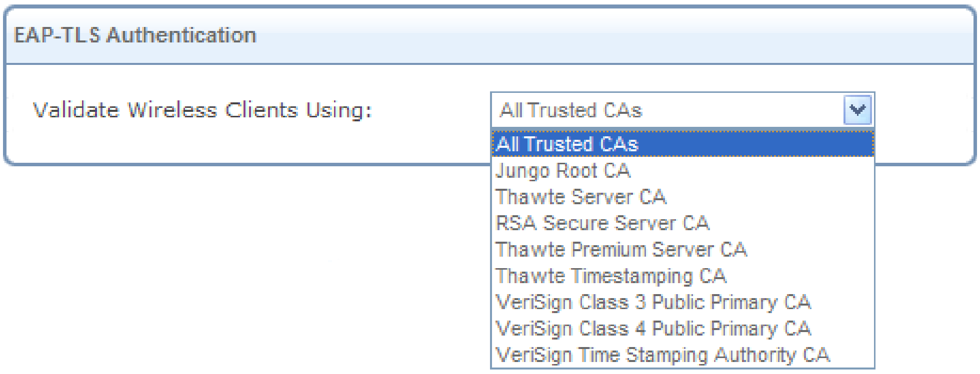


Figure 5.419 EAP-TLS Authentication

5.12.3.3 Connecting Windows Clients with RADIUS Authentication

This section describes the methods for connecting a wireless Windows™ client to a RADIUS client gateway, served by a RADIUS server gateway. There are two methods; one uses the EAP PEAP MSCHAP v2 authentication algorithm and the other uses the EAP TLS algorithm. The following must be configured:

- An OpenRG gateway serving as a RADIUS server
- An OpenRG gateway serving as a RADIUS client
- A Windows computer serving as a wireless client

Configure the OpenRG RADIUS server as described earlier (refer to Section 5.12.3.1 [301]). Next, configure the OpenRG RADIUS client as follows:

1. Access the LAN Wireless network connection settings from the 'Network Connections' link in the 'System' screen, and select the 'Wireless' tab.

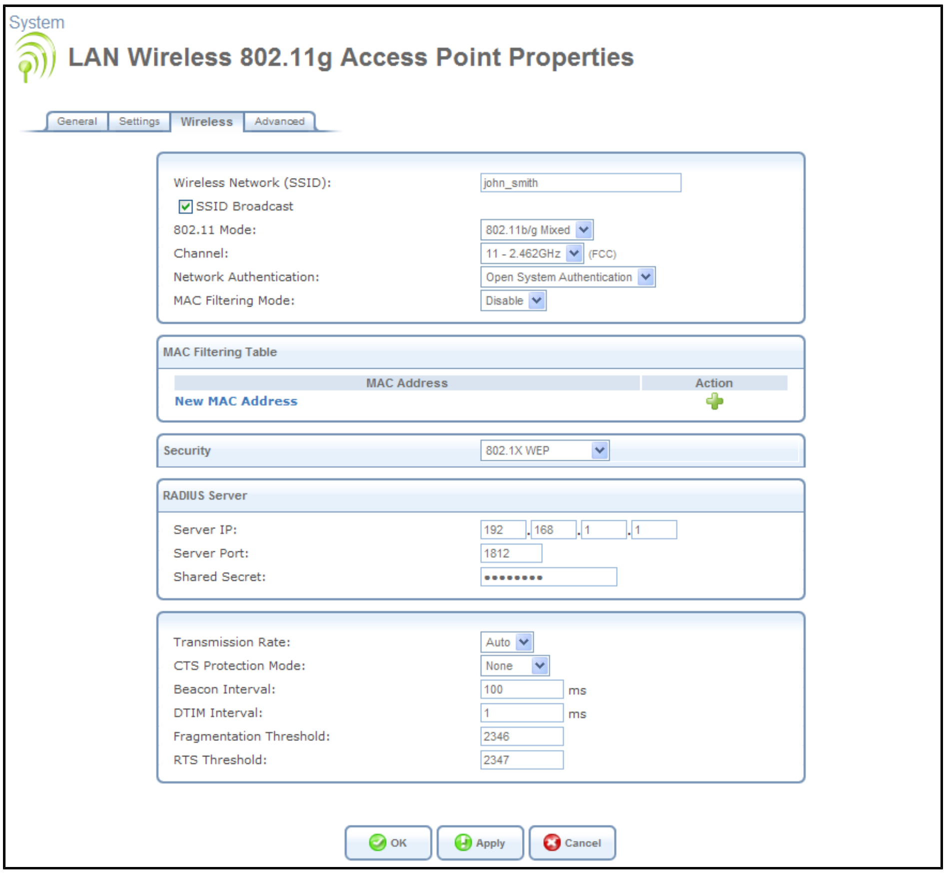


Figure 5.420 LAN Wireless Settings

You may change your wireless network's name (SSID) from the default "openrg" to something more personal (in this example, "john_smith").

2. In the 'Security' section, select either 802.1X WEP or WPA. If you selected WPA, select 802.1X as the authentication method. Note that when selecting WPA, both WPA and WPA2 are supported.

3. In the 'RADIUS Server' section, enter the IP address and shared secret of the gateway serving as a RADIUS server (192.168.1.1), in their respective fields.

4. Click 'OK' to save the settings.

The configuration of the wireless client differs a little between the two algorithms. Start the configuration by performing the following:

1. Access the Windows 'Network Connections' utility and double-click the wireless network connection icon. The 'Wireless Network Connection' window displays the wireless networks in range.

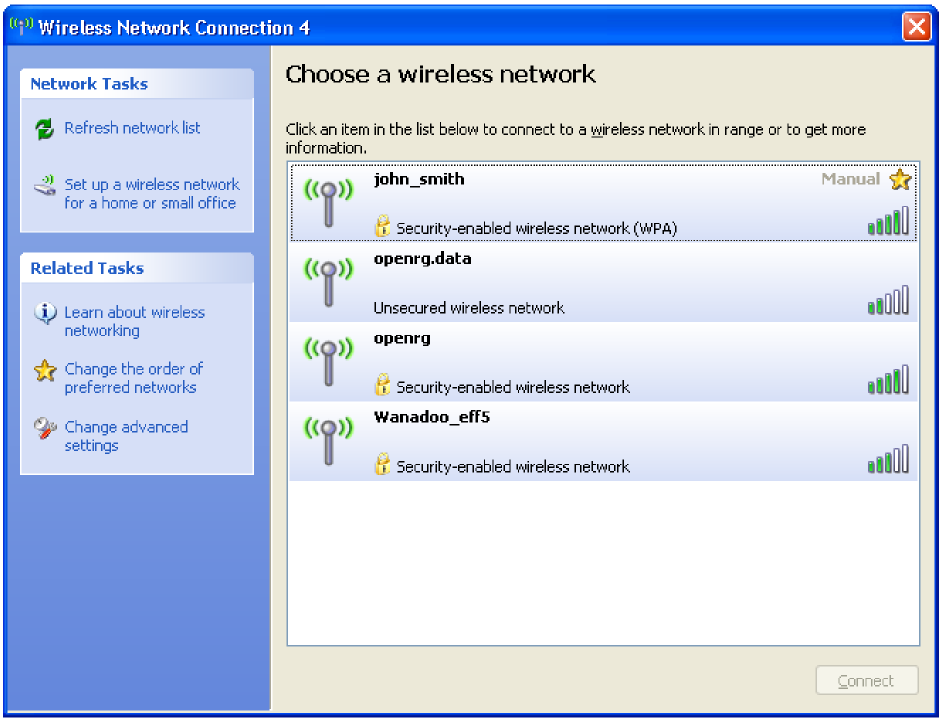


Figure 5.421 Wireless Network Connection Window

2. Click your wireless network entry and then click the 'Change advanced settings' link at the bottom of the side-bar (under "Related Tasks"). The 'Wireless Network Connection Properties' window appears. Click its 'Wireless Networks' tab.

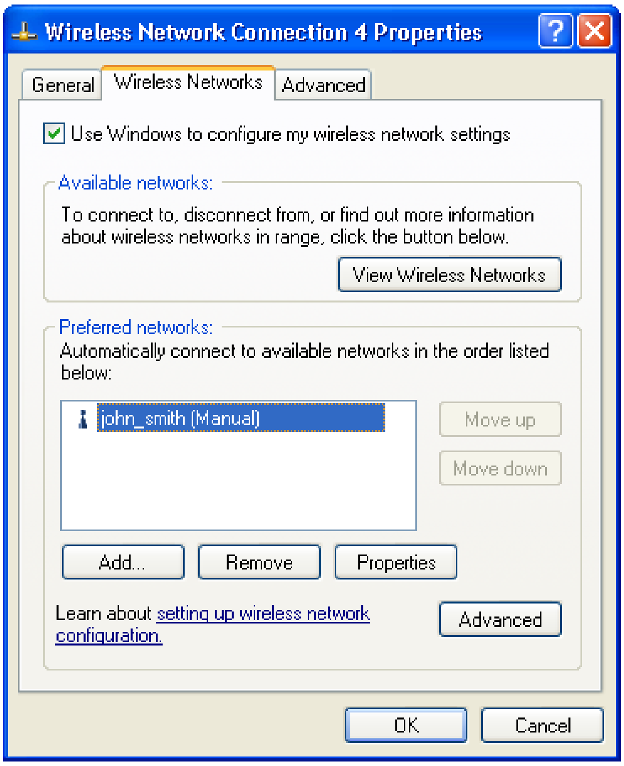


Figure 5.422 Wireless Network Connection Properties Window

3. Click your wireless network entry and then click 'Properties'. The connection's properties window appears.

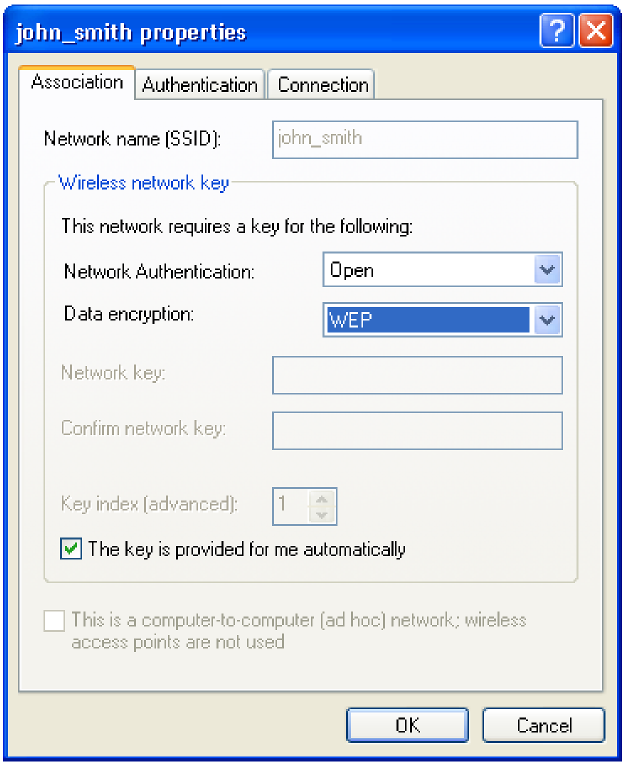


Figure 5.423 Connection Properties Window

4. Verify that your chosen data encryption method is selected. For example, if you had configured the wireless connection (in the RADIUS client) with 802.1X WEP, the 'Data encryption' drop-down menu should display "WEP".

5. Verify that "The key is provided for me automatically" check box is selected.

6. Click the 'Authentication' tab. Verify that the 'Enable IEEE 802.1x' check box is selected.

The procedure now changes according to the algorithm you wish to use.

- With the **EAP PEAP MSCHAP v2** algorithm, negotiation is performed using a server's certificate and a client's user name and password.

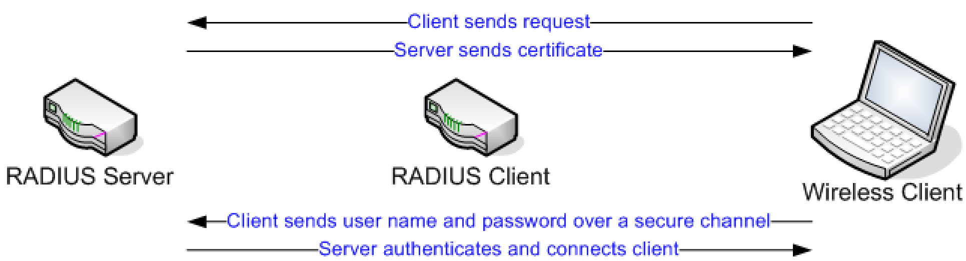


Figure 5.424 Negotiation with the EAP PEAP MSCHAP v2 Algorithm

To use this algorithm, perform the following. For the EAP TLS algorithm, refer to diagram 'Negotiations with the EAP TLS Algorithm'.

1. In the 'Authentication' tab, select the 'Protected EAP (PEAP)' option.

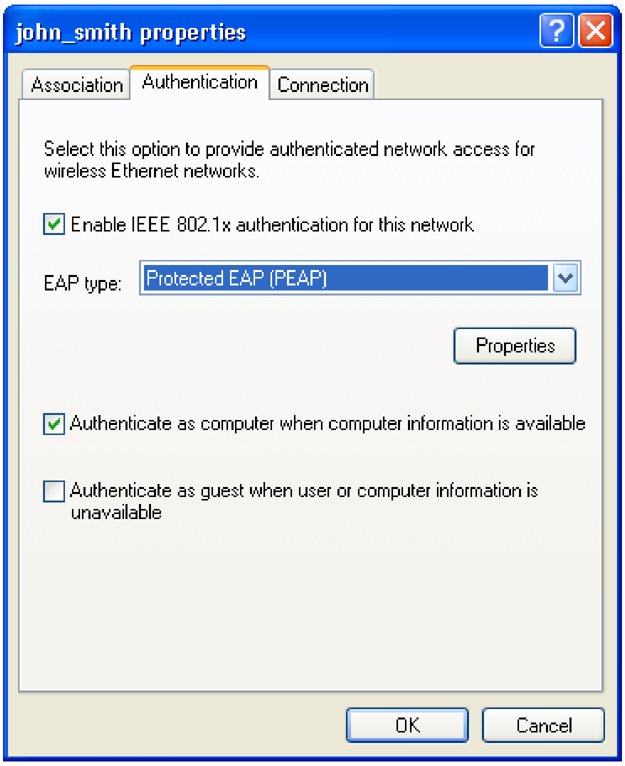


Figure 5.425 Connection Properties Window – EAP PEAP Algorithm

2. Click 'Properties'. The 'Protected EAP Properties' window appears.

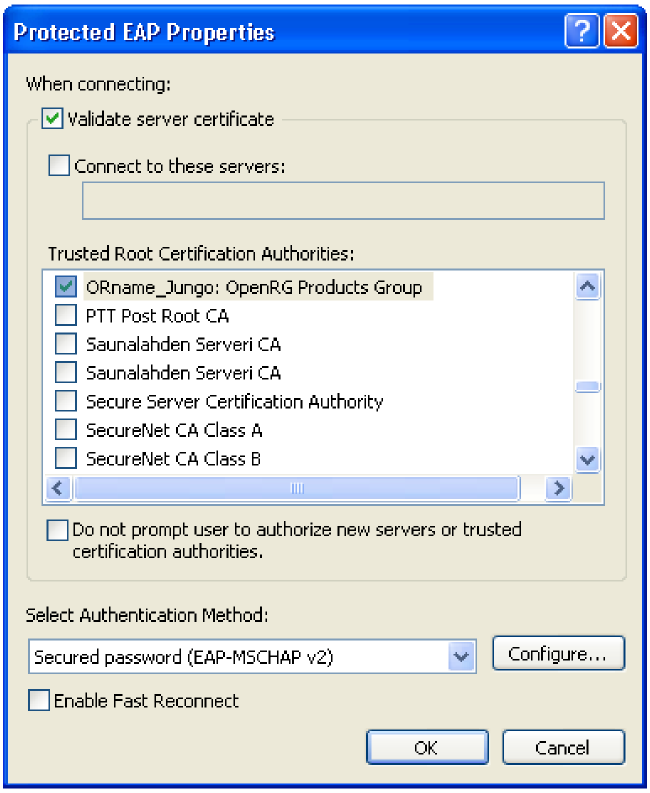


Figure 5.426 Protected EAP Properties

3. Verify that the 'Validate server certificate' check box is selected.

4. Next, you must select a Certificate Authority (CA) by which Windows will verify the RADIUS server. In order for OpenRG's CA to appear in the 'Trusted Root Certification Authorities' list as depicted in Figure 5.426, you must first load the certificate information from the OpenRG RADIUS server to Windows. Perform the following:

   a. In the OpenRG RADIUS server WBM, click the 'Certificates' icon in the 'Advanced' screen. The 'Certificates' screen appears, displaying OpenRG's default certificate under the 'OpenRG's Local' tab.

Figure 5.427 Certificates

   b. Click the action icon of the certificate entry, and select 'Open' in the download dialogue window. The 'Certificate' window appears.

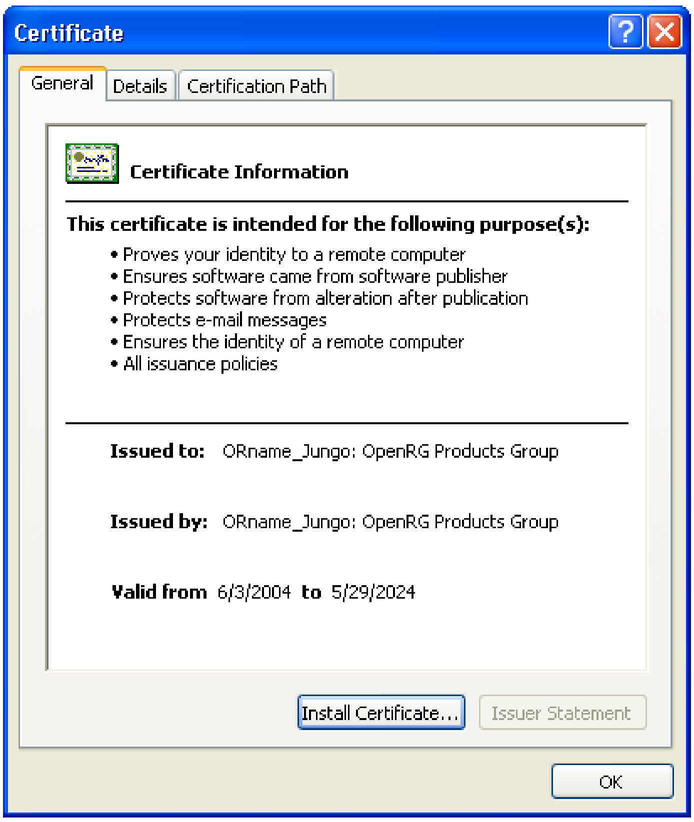


Figure 5.428 Certificate

c. Click 'Install Certificate...'. The 'Certificate Import Wizard' commences. Click 'Next', and select the 'Place all certificates in the following store' option. Click 'Browse' to select the 'Trusted Root Certification Authorities' certificate store.

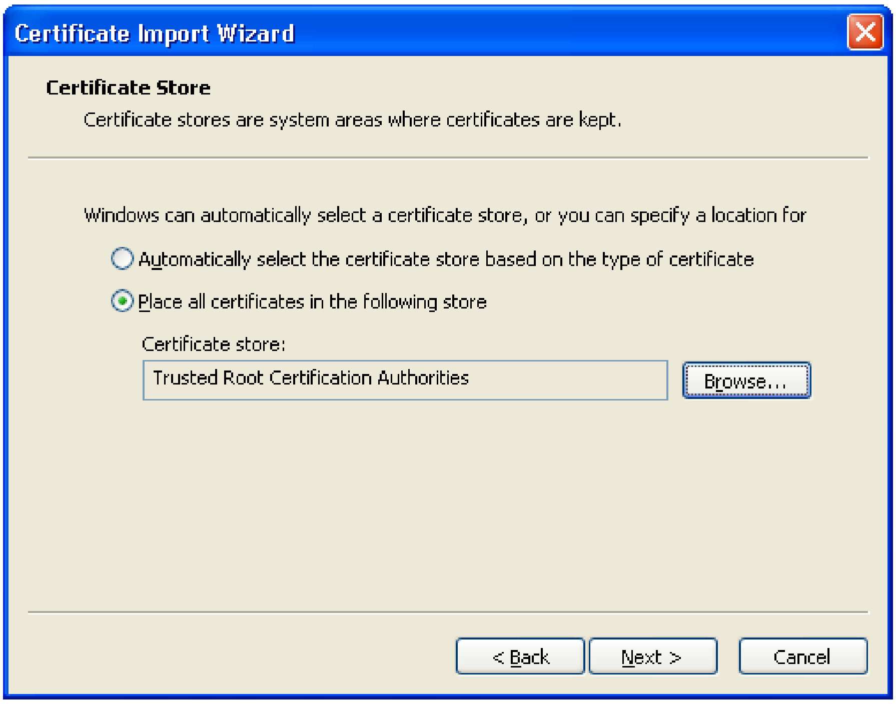


Figure 5.429 Certificate Import Wizard

d. Complete the wizard (click 'Next' and then 'Finish').

5. Back in the 'Protected EAP Properties' window (see Figure 5.426), select the OpenRG CA in the 'Trusted Root Certification Authorities' list.

6. Verify that the "Secured password (EAP-MSCHAP v2)" option is selected in the 'Select Authentication Method' drop-down list, and click 'Configure...'.

7. Uncheck the 'Automatically use my Windows logon name and password' option in the dialogue window, and click 'OK'.

Figure 5.430 EAP MSCHAPv2 Properties

8. Click 'OK' on all open configuration windows.

To connect to the wireless network, click your wireless network entry in the 'Wireless Network Connection' window (see Figure 5.421), and then click 'Connect'. The following message bubble appears.

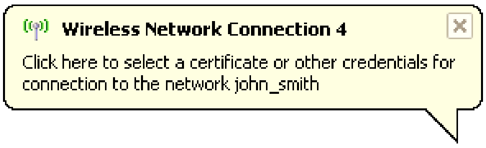


Figure 5.431 Wireless Network Connection Message

Click the bubble. The 'Enter Credentials' window appears.

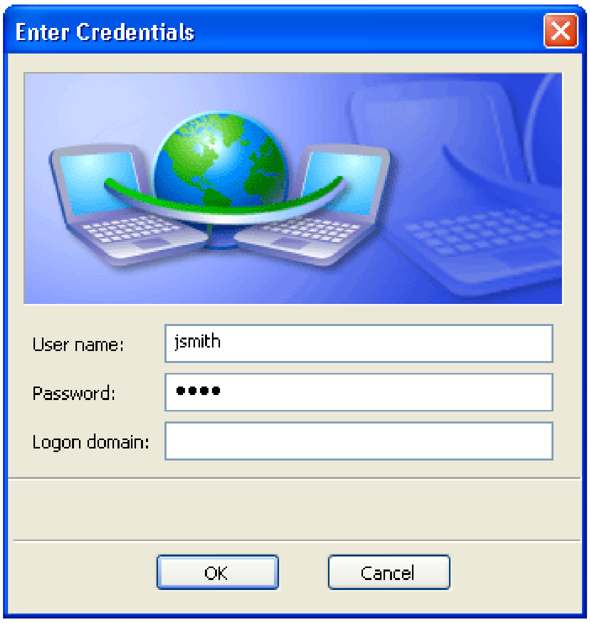


Figure 5.432 Enter Credentials

Enter a user name and password of a user with administrative permissions, predefined in the OpenRG RADIUS server users' list (leave the 'Logon domain' field empty). The wireless connection is now authenticated and established.

- With the **EAP TLS** algorithm, negotiation is performed using both server and client certificates.

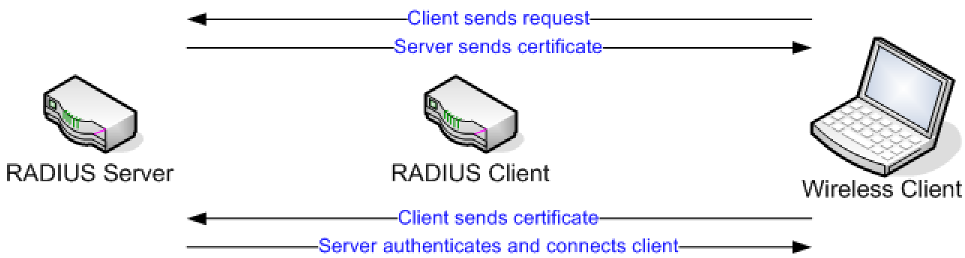


Figure 5.433 Negotiation with the EAP TLS Algorithm

To use this algorithm, perform the following.

1. In the 'Authentication' tab, select the 'Smart Card or other Certificate' option.

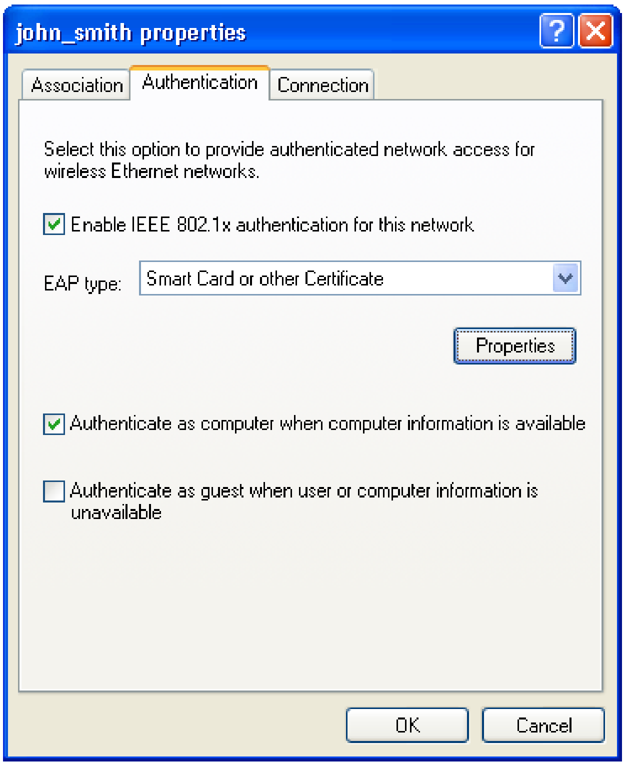


Figure 5.434 Connection Properties Window – EAP TLS Algorithm

2. Click 'Properties'. The 'Smart Card or other Certificate Properties' window appears.

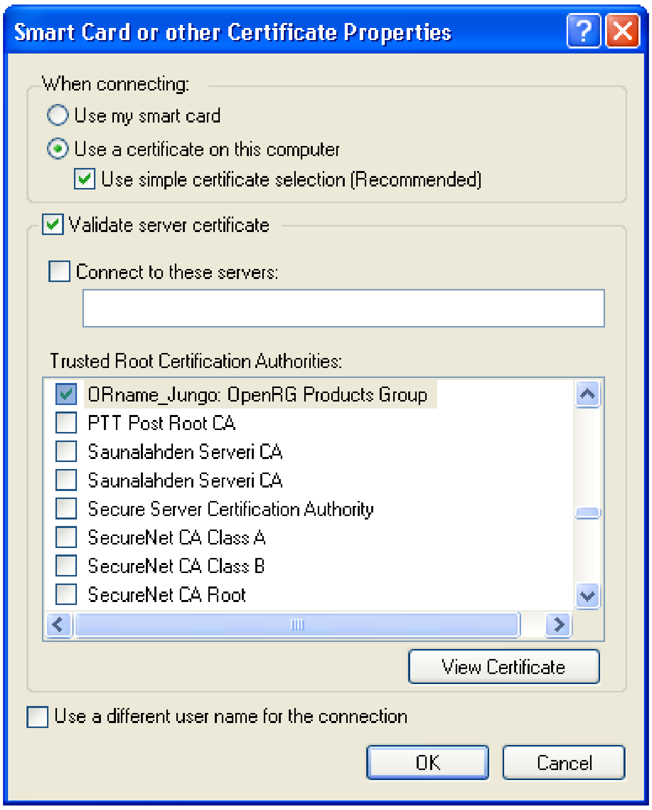


Figure 5.435 Smart Card or other Certificate Properties

3. Verify that the 'Validate server certificate' check box is selected.

4. Verify that the 'Connect to these servers' check box is not selected.

5. Next, you must select a Certificate Authority (CA) by which Windows will verify the RADIUS server. In order for OpenRG's CA to appear in the 'Trusted Root Certification Authorities' list as depicted in Figure 5.435, you must first load the certificate information from the OpenRG RADIUS server to Windows. This procedure is identical to the one described in the EAP PEAP MSCHAP v2 configuration above.

6. Select the OpenRG CA in the 'Trusted Root Certification Authorities' list.

7. Click 'OK' on all open configuration windows.

Since EAP TLS uses certificates for verification of both the server and the client, an additional certificate and private key must be made available for verification of the Windows client. These are commonly available in a **.p12** file, which can be obtained from a certificate authority such as Verisign™, and should be placed on the Windows client. A certificate that authorizes these two must then be saved on the RADIUS server. After obtaining the **.p12** file, save it on the Windows client and perform the following:

1. Load the **.p12** file.

   a. Double-click the .p12 file. The 'Certificate Import Wizard' commences.

   b. Click 'Next', and enter the private key's password.

   c. Click 'Next', and select the 'Place all certificates in the following store' option. Click 'Browse' to select the 'Personal' certificate store.

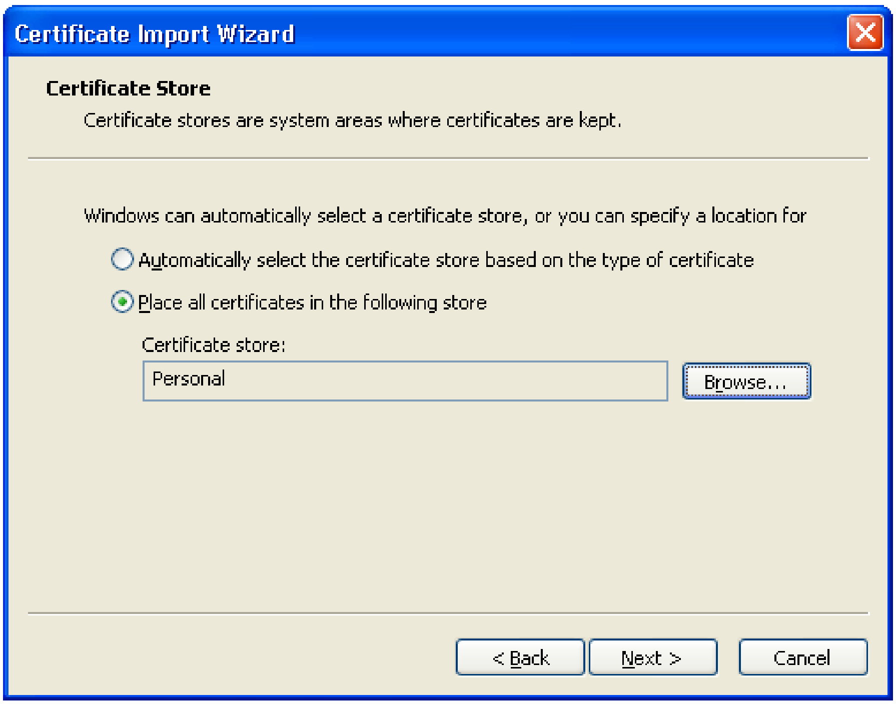


Figure 5.436 Certificate Import Wizard

d. Complete the wizard.

2. Load the authorization certificate to the RADIUS server. Note that either this certificate, or "All Trusted CAs", should be selected in the 'EAP-TLS Authentication' section of the 'RADIUS Server' screen, as described in Section 5.12.3.2 [302].

   a. In the OpenRG RADIUS server WBM, click the 'Certificates' icon in the 'Advanced' screen. The 'Certificates' screen appears. Click the 'CA's' tab.

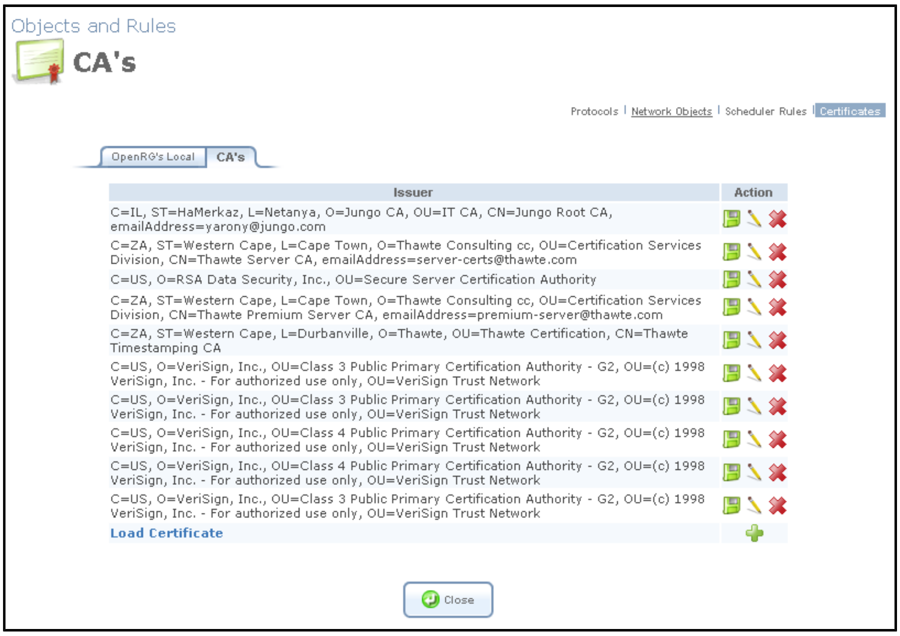


Figure 5.437 CA's

   b. Click 'Load Certificate' and then 'Browse' to locate the certificate file.

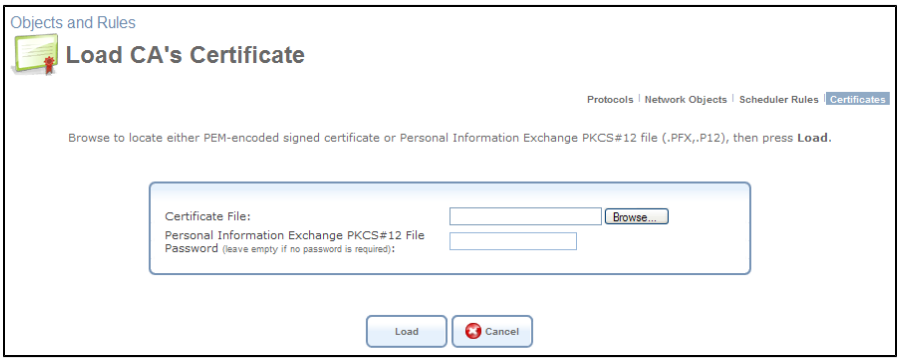


Figure 5.438 Load CA's Certificate

   c. Click 'Load'. The certificate is added to the list in the 'CA's' screen.

To connect to the wireless network, click your wireless network entry in the 'Wireless Network Connection' window (see Figure 5.421), and then click 'Connect'. A confirmation screen appears, informing of the RADIUS server's certificate. Accept the certificate to establish the connection.

6

System

6.1 Viewing the System Information

The 'Overview' screen (see Figure 6.1) displays the gateway's software and hardware characteristics, as well as its uptime.

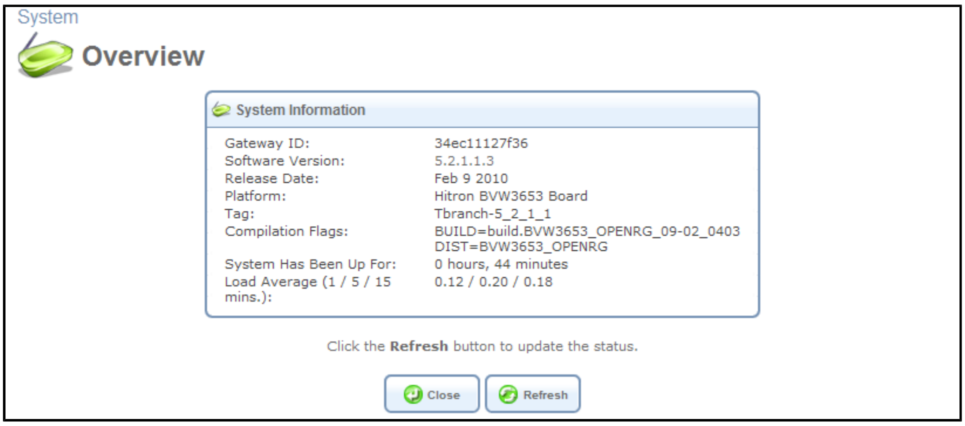


Figure 6.1 System Overview

6.2 Settings

6.2.1 Overviewing and Configuring System Settings

The 'System Settings' screen enables you to configure various system and management parameters.

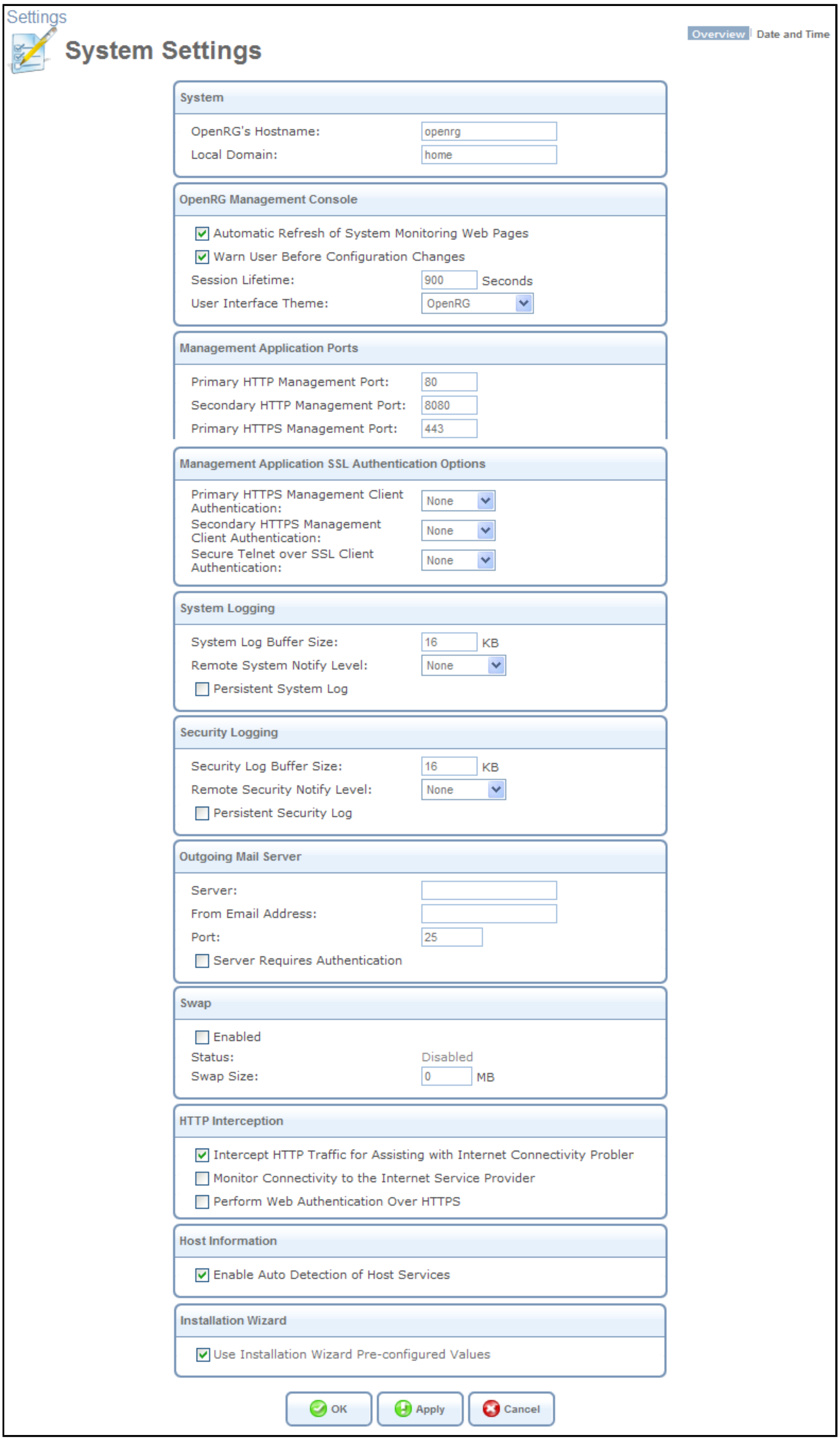


Figure 6.2 System Settings

System Configure general system parameters.

- **OpenRG's Hostname** Specify the gateway's host name. The host name is the gateway's URL address.
- **Local Domain** Specify your network's local domain.

OpenRG Management Console Configure Web-based management settings.

- **Automatic Refresh of System Monitoring Web Pages** Select this check-box to enable the automatic refresh of system monitoring web pages.
- **Warn User Before Network Configuration Changes** Select this check-box to activate user warnings before network configuration changes take effect.
- **Session Lifetime** The duration of idle time (in seconds) in which the WBM session will remain active. When this duration times out, the user will have to re-login.
- **User Interface Theme** You can select an alternative GUI theme from the list provided.

Management Application Ports Configure the following management application ports:

1. Primary/secondary HTTP ports
2. Primary/secondary HTTPS ports
3. Primary/secondary Telnet ports
4. Secure Telnet over SSL port
5. Jungo.net Port
6. Jungo.net SSL Port

> Note: You can selectively enable these management application ports in the 'Remote Administration' screen (for more information, refer to Section 6.7.3).

Management Application SSL Authentication Options Configure the remote client authentication settings, for each of the following OpenRG management options:

- Primary HTTPS Management Client Authentication
- Secondary HTTPS Management Client Authentication
- Secure Telnet over SSL Client Authentication

The applied authentication settings can be either of the following:

- **None** The client is not authenticated during the SSL connection. Therefore, the client does not need to have a certificate recognized by OpenRG, which can be used for authentication (for more information about certificates, refer to Section 6.9.4). This is the default setting for all of the mentioned management options.

- **Required** The client is required to have a valid certificate, which is used instead of the regular login procedure. If the client does not have such a certificate, the connection is terminated.

- **Optional** If the client has a valid certificate, it may be used for authentication instead of the regular login procedure. This means that in case of the HTTPS management session, the user, having a valid certificate, directly accesses the 'Network Map' screen of OpenRG's WBM.

  In case of the secure Telnet connection, the user, having a valid certificate, directly accesses OpenRG's CLI prompt. To learn how to establish a secure Telnet connection to OpenRG, refer to Section 6.7.3. Note that the 'Common Name' (**`CN`**) parameter in the **`Subject`** field of a client's certificate should contain an existing username, to which administrative permissions are assigned.

System Logging Configure system logging parameters. You can view the system log in the 'System Log' screen under 'Monitor' (refer to Section 6.5.3).

- **System Log Buffer Size** Set the size of the system log buffer in Kilobytes.

- **Remote System Notify Level** By default, the 'None' option is selected, which means that OpenRG will not send notifications to a remote host. To activate the feature, select one of the following notification types:

  - Error
  - Warning
  - Information

  The screen refreshes, displaying the 'Remote System Host IP Address' field.

  Figure 6.3 Remote System Host IP Address

  Enter the remote host's IP address and click 'Apply'.

> Note: If you would like to view OpenRG's system logs on a LAN host, you must first install and run the syslog server.

- **Persistent System Log** Select this check box to save the system log to the Flash---the gateway's permanent memory. This will prevent the system log from being erased when the gateway reboots. Note that by default, this check box is deselected.

Security Logging Configure security logging parameters.

- **Security Log Buffer Size** Set the size of the security log buffer in Kilobytes.

- **Remote Security Notify Level** The remote security notification level can be one of the following:
  - None
  - Error
  - Warning
  - Information
- **Persistent Security Log** Select this check box to save the security log to the Flash. This will prevent the security log from being erased when the gateway reboots. Note that by default, this check box is deselected.

> Note: Do not leave the persistent logging feature enabled permanently, as continuous writing of the log files to the Flash reduces gateway's performance.

Outgoing Mail Server Configure outgoing mail server parameters.

- **Server** Enter the hostname of your outgoing (SMTP) server in the 'Server' field.
- **From Email Address** Each email requires a 'from' address and some outgoing servers refuse to forward mail without a valid 'from' address for anti-spam considerations. Enter a 'from' email address in the 'From Email Address' field.
- **Port** Enter the port that is used by your outgoing mail server.
- **Server Requires Authentication** If your outgoing mail server requires authentication check the 'Server Requires Authentication' check-box and enter your user name and password in the 'User Name' and 'Password' fields respectively.

Swap This feature enables you to free a portion of the RAM by creating a swap file on the storage device connected to OpenRG. This is especially useful for platforms with a small RAM. To activate this feature:

1. Verify that a storage device is connected to OpenRG.
2. Select the 'Enabled' check box.
3. In the 'Swap Size' field, enter a swap file size in megabytes.
4. Click 'Apply'. A swap file is created on the storage device, and the feature's status changes to 'Ready'.

HTTP Interception

- **Intercept HTTP Traffic for Assisting with Internet Connectivity Problems** If the WAN device is physically disconnected or cannot obtain an up and running status (even

if an Internet connection exists), OpenRG will display an attention screen providing troubleshooting options (these options are displayed with distributions containing the "Support Cost Reduction (SCR)" feature; otherwise an explanation of the connection's status is provided).

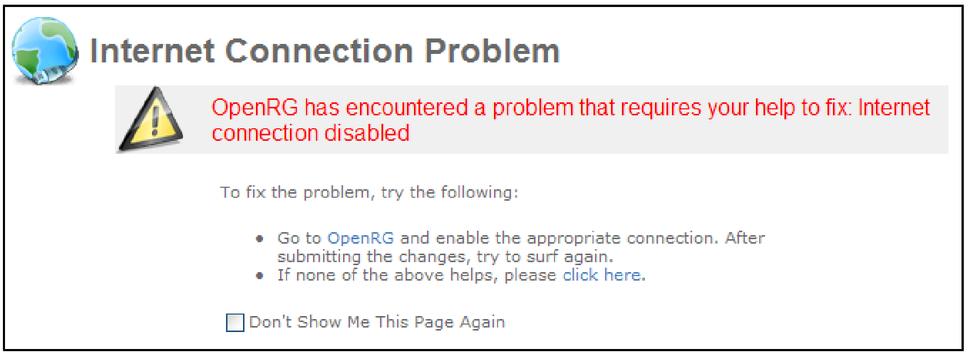


Figure 6.4 Internet Connection Problem

This screen is displayed instead of the browser's standard 'The page cannot be displayed' page.

Note: Selecting the "Don't Show Me This Page Again" option in the attention screen will disable this feature.

- **Monitor Connectivity to the Internet Service Provider** The WAN device can be up and running even if no Internet connection is available (for example, when a static IP address is defined). Select this check box to have OpenRG perform periodic Internet connectivity checks and display the attention screen if the connection becomes unavailable.

Note: Selecting the "Don't Show Me This Page Again" option in the attention screen will disable this feature.

- **Perform Web Authentication Over HTTPS** Select this check box to secure OpenRG's interception page, in order to protect the required login details. Web authentication will be performed through an HTTPS WBM page.

Host Information OpenRG can auto-detect its LAN hosts' properties, available services, traffic statistics, and connections (for more information refer to Section 4.1). To enable this feature, select its check box.

Installation Wizard Select the 'Use Installation Wizard Pre-configured Values' check box to have the wizard skip the steps for which parameters had been preconfigured and saved in factory settings file (**rg_factory**).

6.2.2 Setting the Date and Time

The 'Date and Time' menu item enables you to configure your gateway's time, date, time zone and daylight saving (summer time) settings.

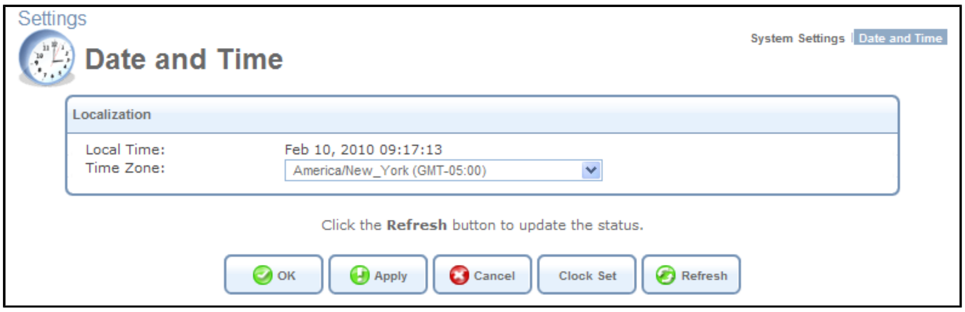


Figure 6.5 Date and Time Settings

- **Setting Your Local Time Zone**
  From the 'Time Zone' drop-down menu, select a time zone that corresponds to your current location. If you wish to manually define your time zone settings, select the 'Other' option. The screen refreshes, displaying the 'GMT Offset' field.

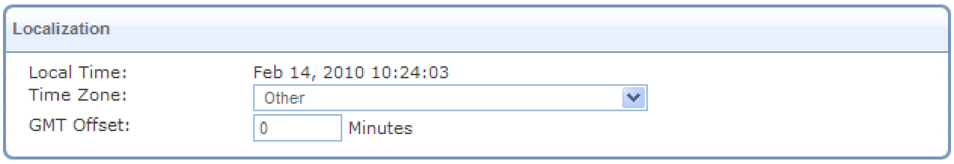


Figure 6.6 Local Time Zone – GMT Offset

This field enables you to manually adjust your local time's offset from the Greenwich Mean Time (GMT).

- **Configuring the Daylight Saving Settings**
  OpenRG automatically detects the daylight saving settings of a large number of time zones, by using its internal time zone database. There are several time zones, however, for which the daylight saving settings have not been preset on OpenRG, as they may vary occasionally. In case the daylight saving settings of your selected time zone may periodically vary, the following fields appear, enabling you to manually configure your local daylight saving time.

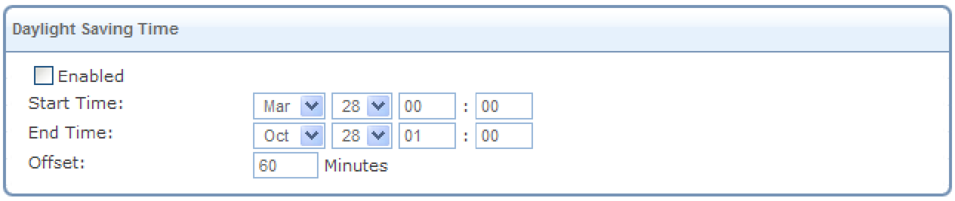


Figure 6.7 Daylight Saving Settings

Enabled Select this check box to automatically enable the daylight saving mode during the period specified below.

Start A date and time when your time zone's daylight saving period starts.

End A date and time when your time zone's daylight saving period ends.

Offset A daylight saving time offset from the standard (winter) time.

- If you want the gateway to periodically perform an automatic time update, proceed as follows:

    1. Select the 'Enabled' check box under the 'Automatic Time Update' section.

    2. Select the protocol to be used to perform the time update by selecting either the 'Time of Day' or 'Network Time Protocol' radio button.

    3. In the 'Update Every' field, specify the frequency of performing the update.

    4. By default, OpenRG is configured with Jungo's NTP server for testing purposes only. You can define another time server address by clicking the 'New Entry' link at the bottom of the 'Automatic Time Update' section. You can find a list of time server addresses sorted by region at http://www.pool.ntp.org.

In addition, OpenRG can function as a Simple Network Time Protocol (SNTP) server, enabling you to automatically update the time settings of your computers from a single but reliable source. By default, OpenRG's SNTP server is enabled. To synchronize time between the SNTP server and a PC connected to the gateway, perform the following:

1. In the 'Automatic Time Update' section of the 'Date and Time' screen (see Figure 6.5), click the 'Network Time Protocol (NTP)' radio button.

2. Click 'OK' to save the settings.

3. On a PC connected to the gateway, perform the following:

    > Note: The following explanations are based on the Windows XP user interface.

    1. In Control Panel, double-click the 'Date and Time' icon. The 'Date and Time Properties' window appears.

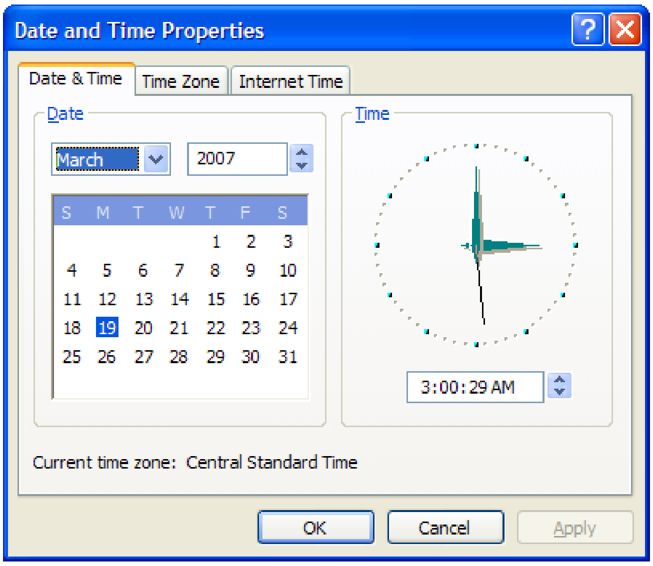


Figure 6.8 Windows – Date and Time Properties

2. Click the 'Internet Time' tab. The window changes to the following.

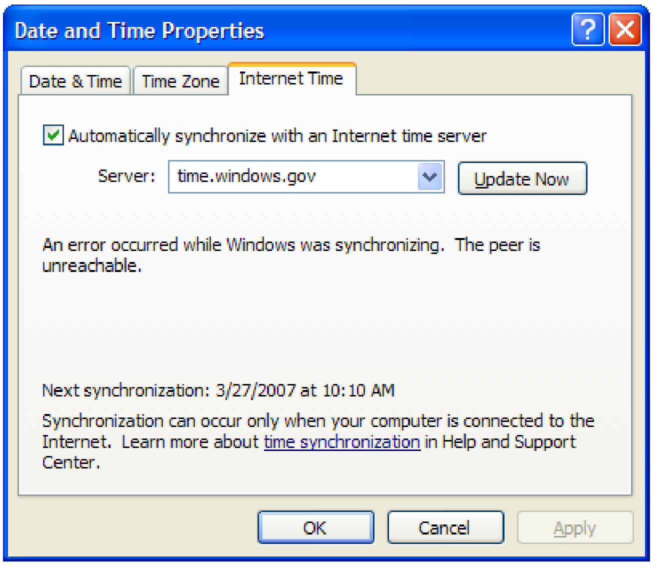


Figure 6.9 Windows – Internet Time Screen

3. In the 'Server' field, enter OpenRG's LAN IP address (The default one is 192.168.1.1).
4. Click 'Update Now'. Windows will synchronize with OpenRG's SNTP server. In addition, Windows will perform a periodical synchronization with the SNTP server.
5. Click 'OK' to save the settings.

6.3 Managing Users

The 'Users' menu item enables you to view and edit the defined user accounts.

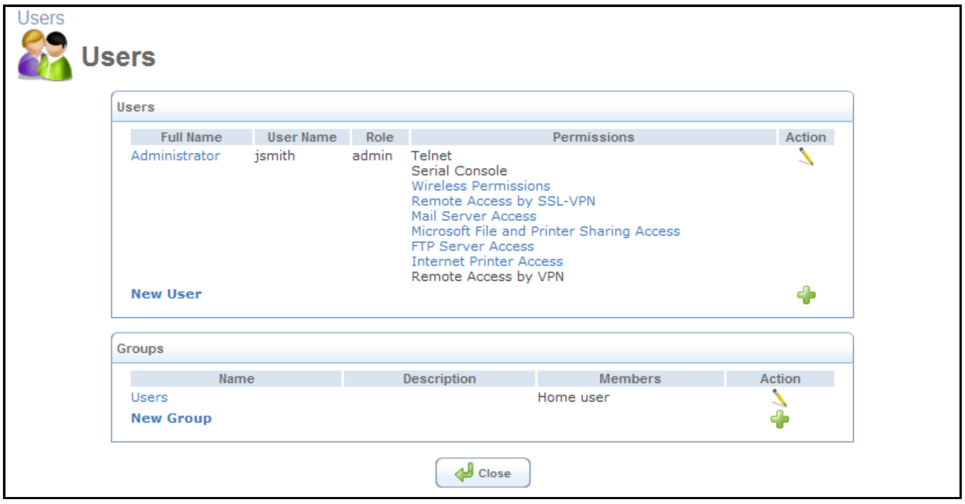


Figure 6.10 Users

By default, only one user account (*Admin*) is available.

6.3.1 Disk Management

Enable User Home Directory By default, this option is selected. When activated, it creates a directory for the user in the 'Home' directory of the system storage area. This directory is necessary when using various applications, such as the mail server. For more information, refer to Section 5.9.7.2.

6.3.2 E-Mail Notification

You can use email notification to receive indications of system events for a predefined severity classification. The available types of events are 'System' or 'Security' events. The available severity of events are 'Error', 'Warning' and 'Information'.

If the 'Information' level is selected, the user will receive notification of the 'Information', 'Warning' and 'Error' events. If the 'Warning' level is selected, the user will receive notification of the 'Warning' and 'Error' events etc.

To configure email notification for a specific user:

- Make sure you have configured an outgoing mail server in 'System Settings'. A click on the 'Configure Mail Server' link will display the 'System Settings' screen where you can configure the outgoing mail server.
- Enter the user's email address in the 'Address' field of the 'Email' section.
- Select the 'System' and 'Security' notification levels in the 'System Notify Level' and 'Security Notify Level' drop-down menu respectively.

6.3.3 Group Settings

You may assemble your defined users into different groups, based on different criteria—for example, home users versus office users. By default, new users will be added to the default group "Users". To add a new group, click the 'New Group' link. The 'Group Settings' screen appears.

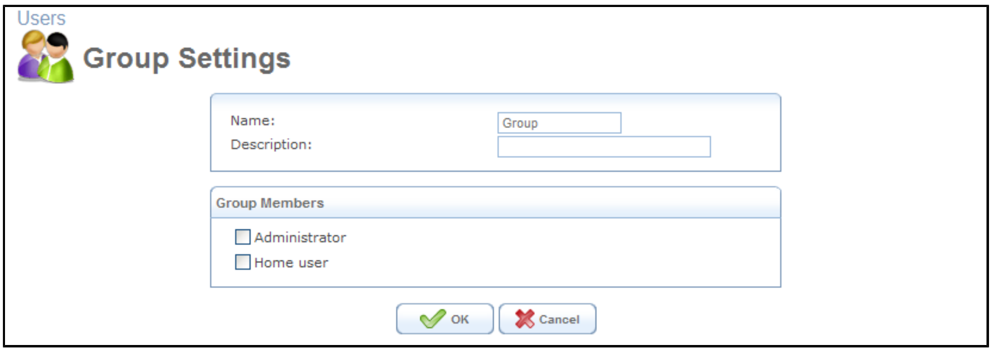


Figure 6.11 Group Settings

Name Enter a name for the group of users.

Description You may also enter a short description for the group.

Group Members Select the users that will belong to this group. All users defined are presented in this section. A user can belong to more than one group.

6.3.4 Editing a User's Profile

To edit a user's profile (for example, change the assigned permissions or password), click the user's link or the corresponding action icon (see Figure 6.10). The 'User Settings' screen appears.

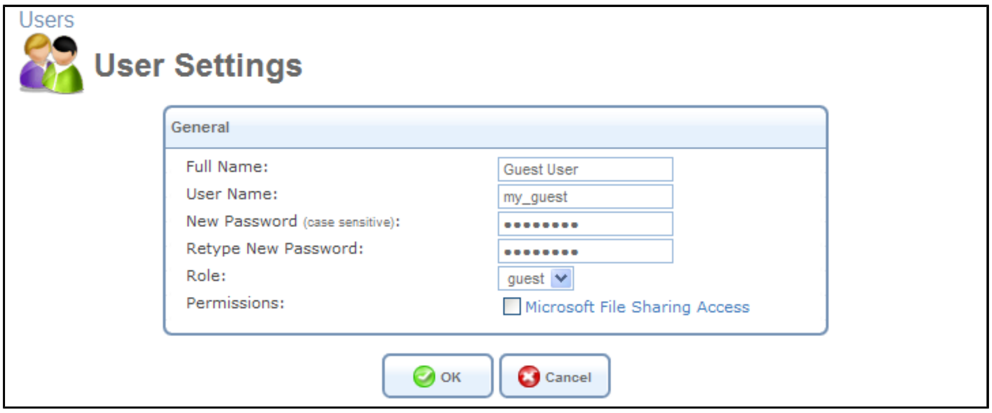


Figure 6.12 User Settings

After making the necessary changes, click 'OK' to save them.

6.4 Network Connections

This chapter describes the different network connections available with OpenRG, as well as the connection types that you can create. OpenRG supports both physical and logical network connections. When clicking the 'Network Connections' menu item under 'System', the 'Network Connections' screen appears, enabling you to configure the various parameters of your physical connections (the LAN and WAN), and create new connections, using tunneling protocols over existing connections (such as PPP and VPN).

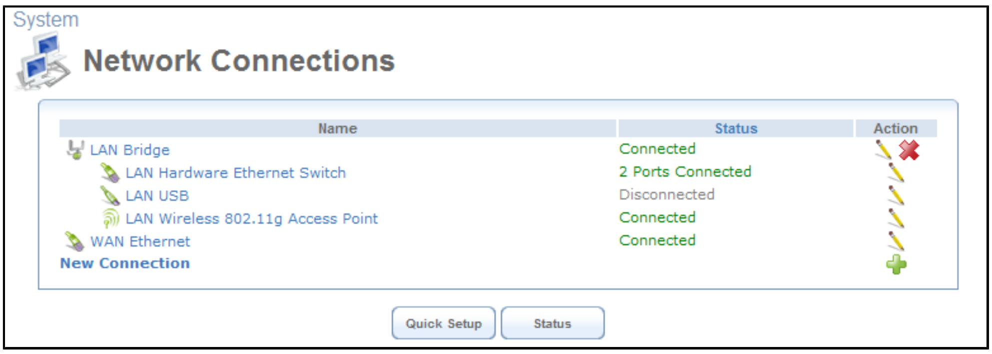


Figure 6.13 Network Connections

Note: Some of the connections described in this chapter may not be available with certain versions of OpenRG.

OpenRG's physical network connections are:

- **LAN** – Creating a home/SOHO network
  - LAN Ethernet (refer to Section 6.4.4).
  - LAN Hardware Ethernet Switch (refer to Section 6.4.3).
  - LAN Wireless 802.11g Access Point (refer to Section 6.4.6).
- **WAN** – Internet Connection
  - WAN Ethernet (refer to Section 6.4.7).

The logical network connections available with OpenRG are:

- **WAN** – Internet Connection
  - Point-to-Point Protocol over Ethernet (refer to Section 6.4.8).
  - Point-to-Point Tunneling Protocol (refer to Section 6.4.11).
  - Layer 2 Tunneling Protocol (refer to Section 6.4.9).
  - WAN-LAN Bridge (refer to Section 6.4.15).
- **Virtual Private Network over the Internet**
  - Layer 2 Tunneling Protocol over Internet Protocol Security (refer to Section 6.4.9).
  - Layer 2 Tunneling Protocol Server (refer to Section 6.4.10).
  - Point-to-Point Tunneling Protocol Virtual Private Network (refer to Section 6.4.11).
  - Point-to-Point Tunneling Protocol Server (refer to Section 6.4.12).
  - Internet Protocol Security (refer to Section 6.4.13).
  - Internet Protocol Security Server (refer to Section 6.4.14).
- **Advanced Connections**
  - Network Bridging (refer to Section 6.4.5 and Section 6.4.15).
  - VLAN Interface (refer to Section 6.4.16).
  - Internet Protocol over Internet Protocol (refer to Section 6.4.17).

- General Routing Encapsulation (refer to Section 6.4.18).

6.4.1 Network Types

Every network connection in OpenRG can be configured to operate in one of three modes: WAN, LAN or DMZ. This provides high flexibility and increased functionality. For example, you may define that a LAN Ethernet connection on OpenRG will operate as a WAN network. This means that all hosts in this LAN will be referred to as WAN computers, both by computers outside OpenRG and by OpenRG itself. WAN and firewall rules may be applied as on any other WAN network.

Another example is a network connection that is defined as a DMZ (Demilitarized) network. Although this network is physically inside OpenRG, it will function as an unsecured, independent network, for which OpenRG merely acts as a router.

6.4.2 Using the Connection Wizard

The logical network connections can be easily created using the Connection Wizard. This wizard consists of a series of management screens, intuitively structured to gather all the information needed to create a logical connection.

6.4.2.1 Creating Connections on an Ethernet Gateway

To initiate a connection setup using the wizard, click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears.

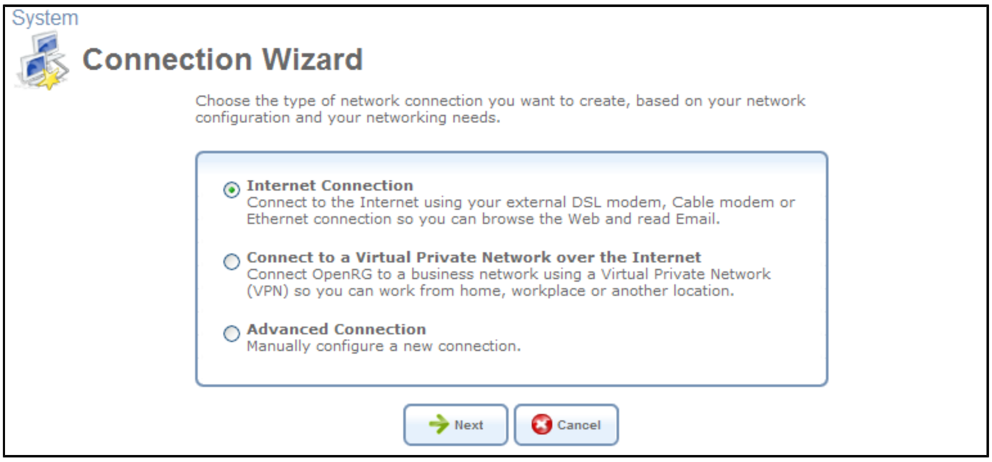


Figure 6.14 Connection Wizard

This screen presents you with the main connection types. Each option that you choose will lead you to further options, adding more information with each step and narrowing down the parameters towards the desired network connection.

- **Internet Connection** – Selecting this option takes you to the 'Internet Connection' screen, enabling you to set up your Internet connection, in one of the available methods.

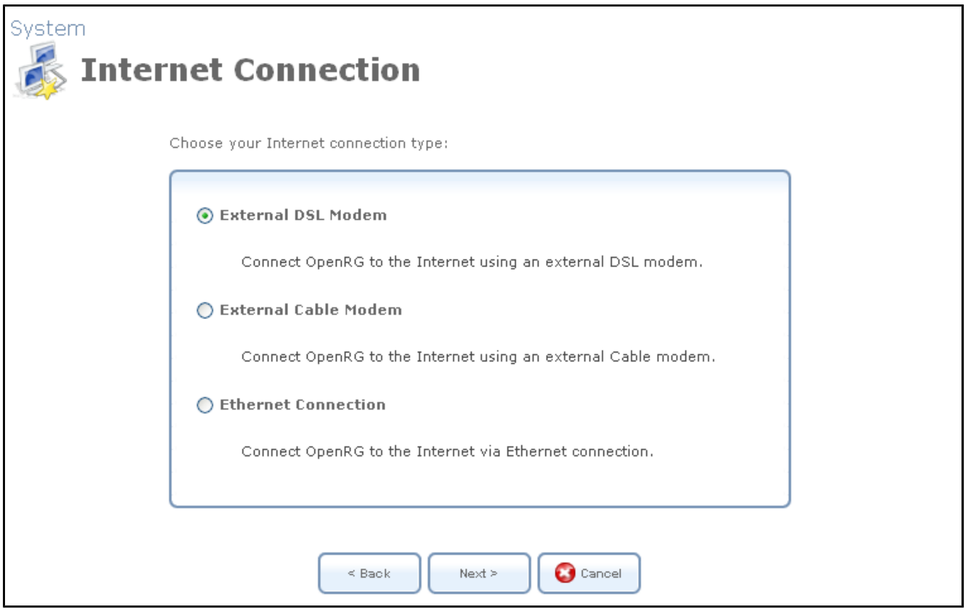


Figure 6.15 Internet Connection Wizard Screen

The Internet connection setup options are depicted in Figure 6.16, where rectangles represent the steps/screens to be taken and ellipses represent the available connections.

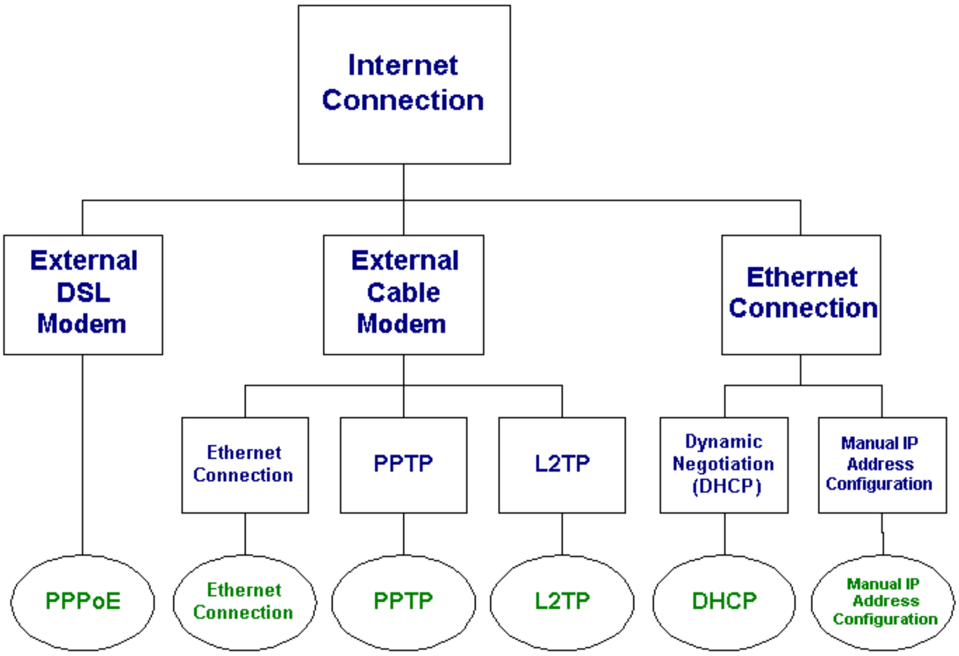


Figure 6.16 Internet Connection Wizard Tree

- **Connect to a Virtual Private Network over the Internet** – Selecting this option takes you to the 'Connect to a Virtual Private Network over the Internet' screen, enabling you to securely connect OpenRG to a business network using a Virtual Private Network (VPN).

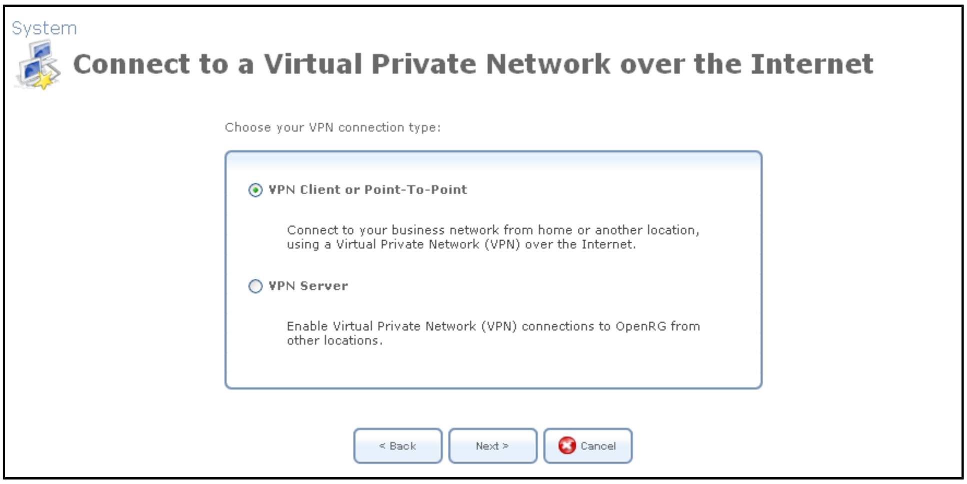


Figure 6.17 VPN Wizard Screen

The VPN setup options are depicted in Figure 6.18, assisting you in choosing a VPN setup mode that suits your needs—either a VPN client or a server.

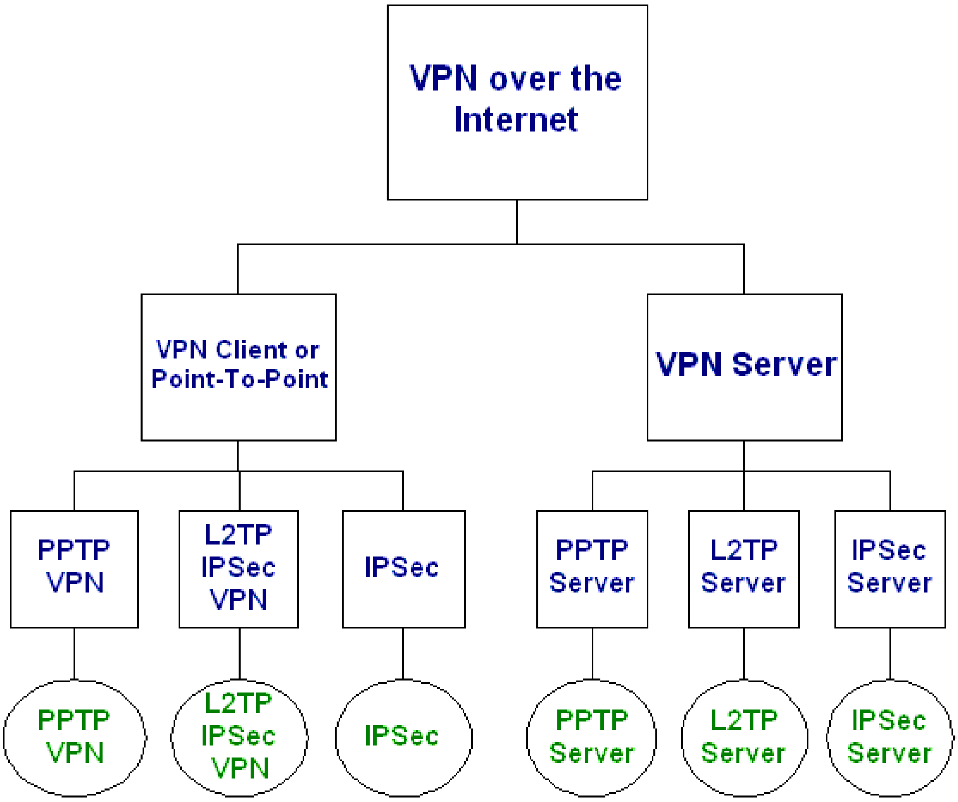


Figure 6.18 VPN Wizard Tree

- **Advanced Connection** – Selecting this option takes you to the 'Advanced Connection' screen, enabling you to select a type of logical network connection setup that you would like to initiate. In addition, it provides a wizard for creating the Network Bridge and VLAN Interface connections.

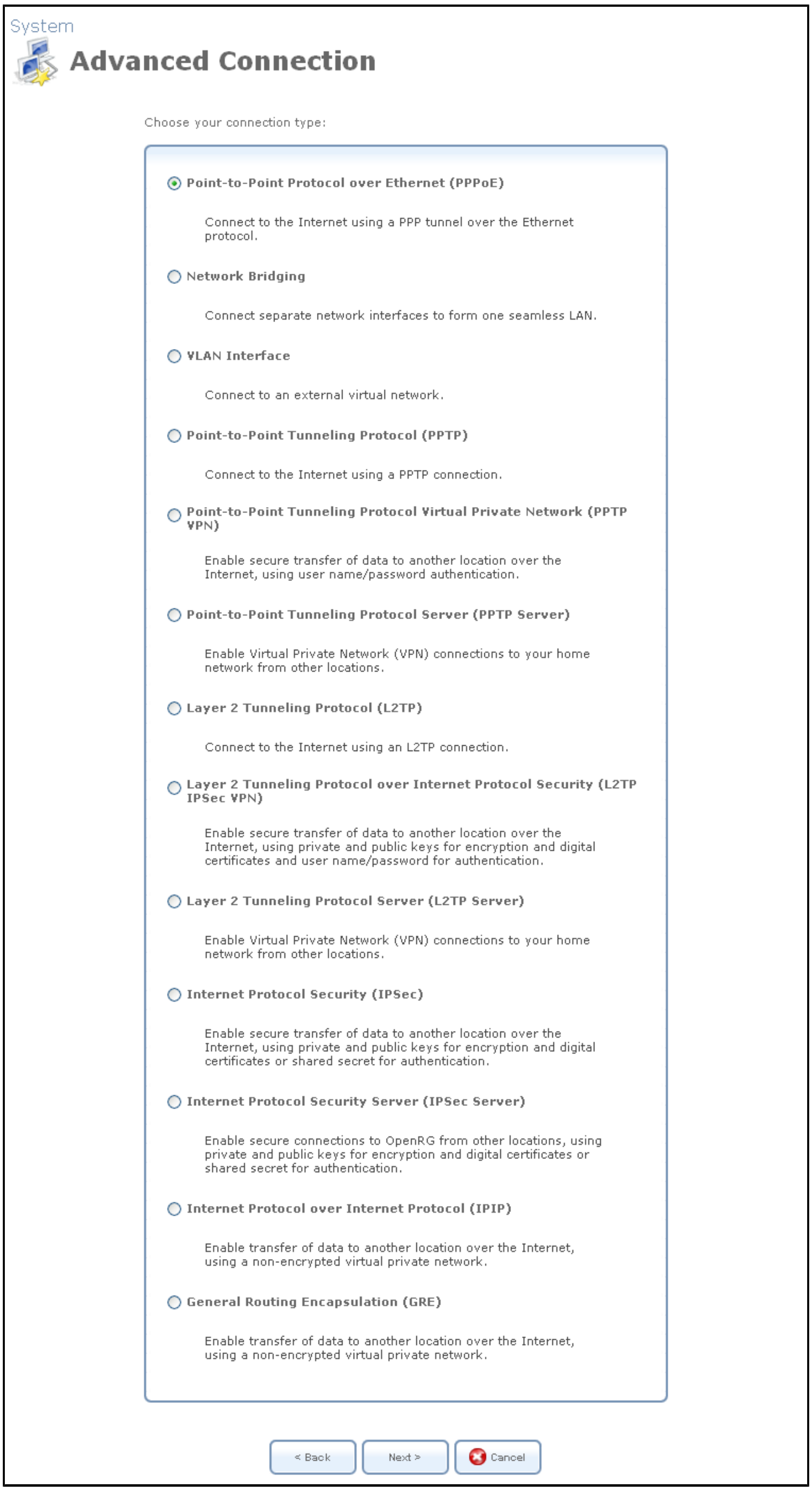


Figure 6.19 Advanced Connection Wizard Screen

The Advanced Connection options are depicted in Figure 6.20.

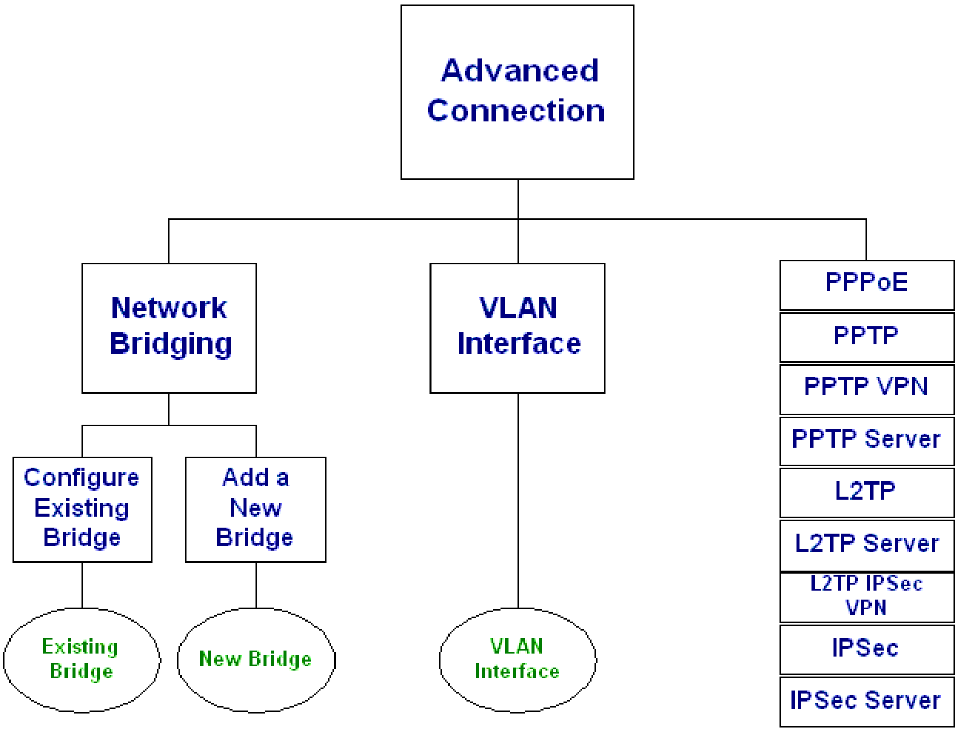


Figure 6.20 Advanced Connection Wizard Tree

6.4.3 Configuring the LAN Hardware Ethernet Switch Settings

The LAN Hardware Ethernet Switch interface represents all of OpenRG's LAN ports. To view and modify the LAN Hardware Ethernet Switch settings, click the 'LAN Hardware Ethernet Switch' link in the 'Network Connections' screen (see Figure 6.13). The 'LAN Hardware Ethernet Switch Properties' screen appears.

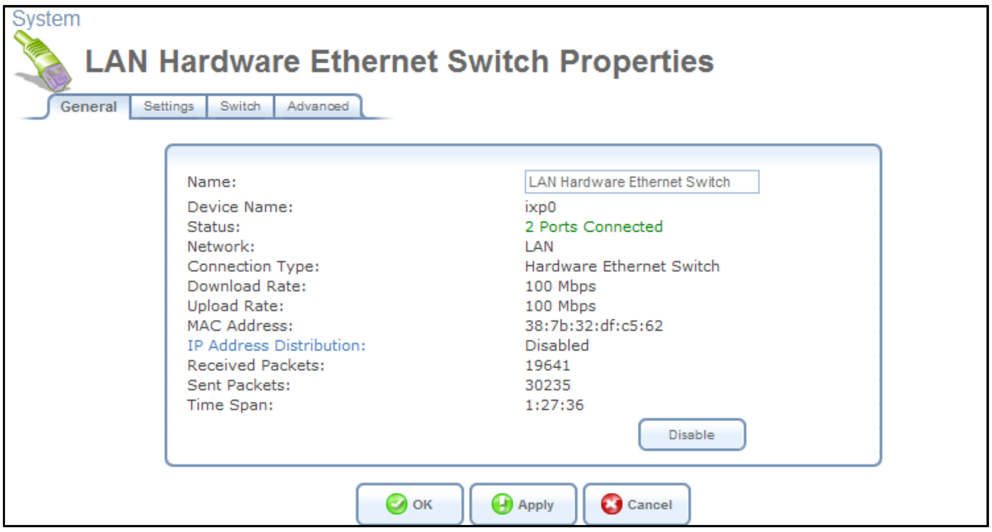


Figure 6.21 LAN Hardware Ethernet Switch Properties

6.4.3.1 General

This sub-tab enables you to view the LAN Hardware Ethernet Switch settings (see Figure 6.21). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.3.2 Settings

This sub-tab displays the connection's general parameters. It is recommended not to change the default values unless you are familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

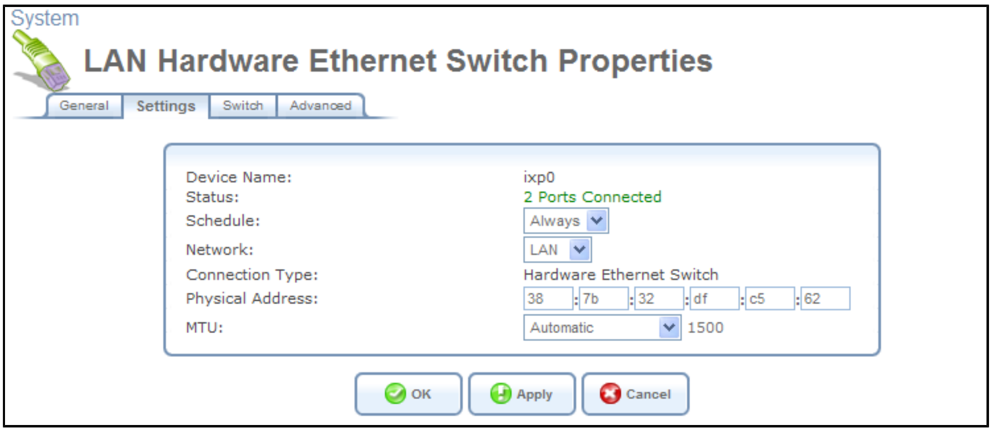


Figure 6.22 Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP

determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

6.4.3.3 Switch

This sub-tab displays the hardware switch ports properties. The switch ports are physical sockets on the board, to which different cables connect. The table in this screen consists of a list of all available ports, their status, and the VLANs of which they are members. Untagged packets (packets with no VLAN tag) that arrive in a port, will be tagged with the VLAN number that appears under the Port VLAN Identifier (PVID) column.

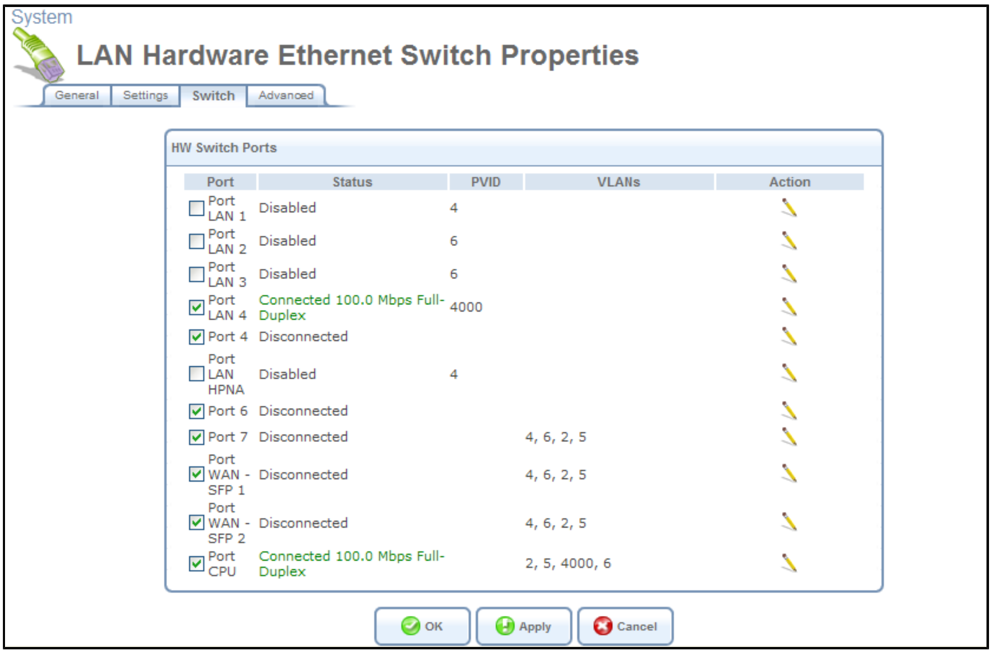


Figure 6.23 Switch

You can edit the configuration of each port. To do so, click a connected port's action icon . The 'Port LAN Settings' screen appears.

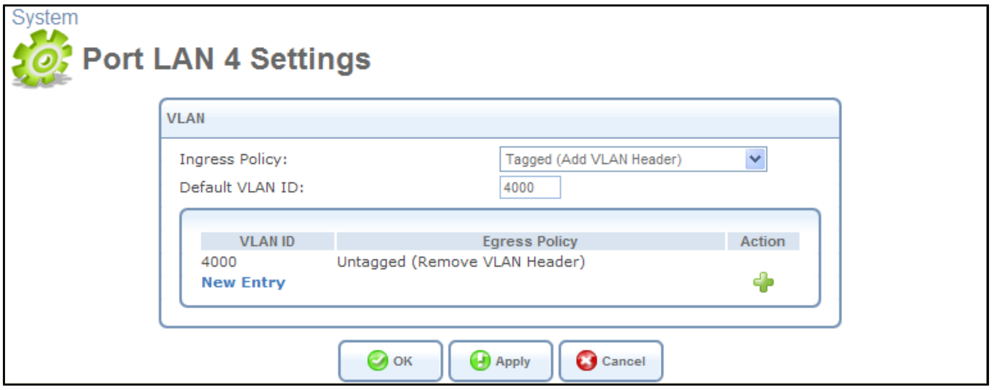


Figure 6.24 Port LAN Settings

Ingress Policy Select whether or not to tag incoming packets with the port's VLAN header. When the 'Tagged (Add VLAN Header)' option is selected, additional fields appear.

Default VLAN ID The port's VLAN identifier. You may add additional identifiers to the VLAN by clicking 'New Entry'.

6.4.3.4 Advanced

This sub-tab enables you to configure the following advanced switch settings.

- **Internet Connection Firewall** Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

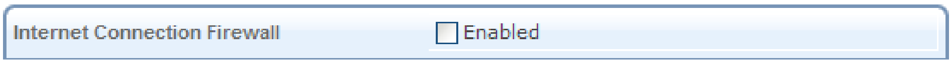


Figure 6.25 Internet Connection Firewall

Internet Connection Fastpath Select this check box to utilize the *Fastpath* algorithm for enhancing packet flow, resulting in faster communication between the LAN and the WAN. By default, this feature is enabled.

Figure 6.26 Internet Connection Fastpath

- **Additional IP Addresses** You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://openrg.home.

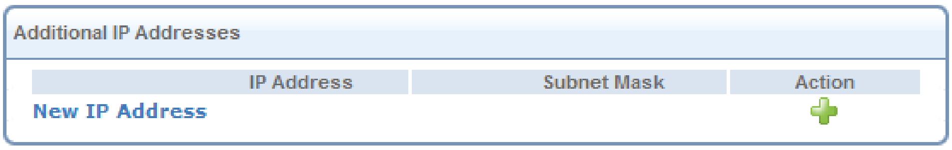


Figure 6.27 Additional IP Addresses

6.4.4 Configuring the LAN Ethernet Settings

The LAN Ethernet connection is available only on gateways that do not have a built-in LAN hardware Ethernet switch. This connection enables you to connect computers to OpenRG using Ethernet cables, either directly or via network hubs and switches.

To view and edit the LAN Ethernet connection settings, click the 'LAN Ethernet' link in the 'Network Connections' screen (see Figure 6.13). The 'LAN Ethernet Properties' screen appears.

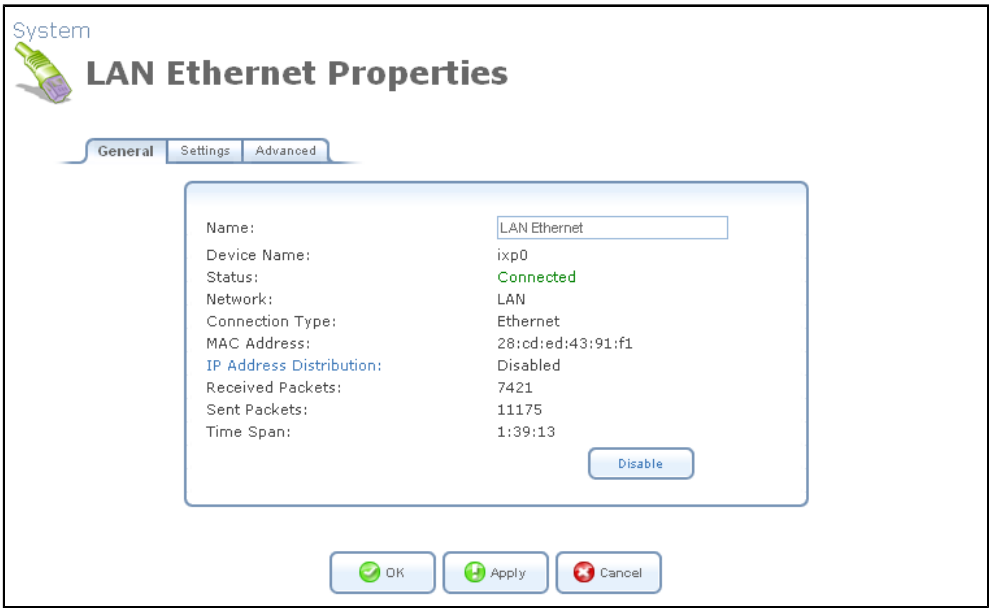


Figure 6.28 LAN Ethernet Properties

6.4.4.1 General

This sub-tab enables you to view a detailed summary of the connection's settings (see Figure 6.28). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.4.2 Settings

This sub-tab enables you to edit the following LAN Ethernet settings.

General This section displays the connection's general parameters. It is recommended not to change the default values unless you are familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

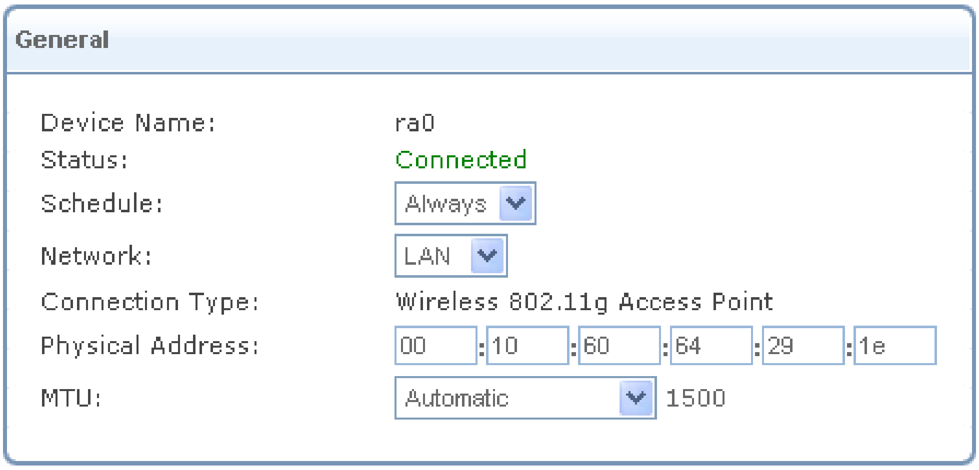


Figure 6.29 General Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

6.4.4.3 Advanced

This sub-tab enables you to edit the advanced LAN Ethernet settings.

- **Internet Connection Firewall** Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

Figure 6.30 Internet Connection Firewall

Internet Connection Fastpath Select this check box to utilize the *Fastpath* algorithm for enhancing packet flow, resulting in faster communication between the LAN and the WAN. By default, this feature is enabled.

Figure 6.31 Internet Connection Fastpath

- **Additional IP Addresses** You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://openrg.home.

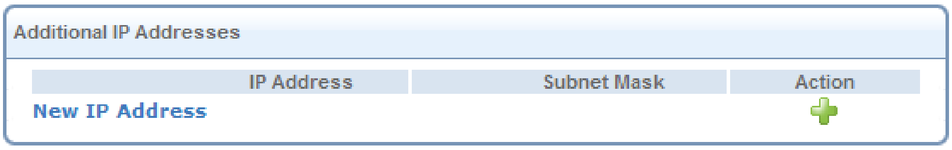


Figure 6.32 Additional IP Addresses

6.4.5 Setting Up a LAN Bridge

The LAN bridge connection is used to combine several LAN devices under one virtual network. For example, creating one network for LAN Ethernet and LAN wireless devices. Note that when a bridge is removed, its formerly underlying devices inherit the bridge's DHCP settings. For example, the removal of a bridge that is configured as DHCP client, automatically configures the LAN devices formerly constituting the bridge as DHCP clients, with the exact DHCP client configuration.

6.4.5.1 Creating a LAN Bridge Connection

To create a new bridge or configure an existing one, perform the following:

1. In the 'Network Connections' screen under 'System' (see Figure 6.13), click the 'New Connection' link. The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears.

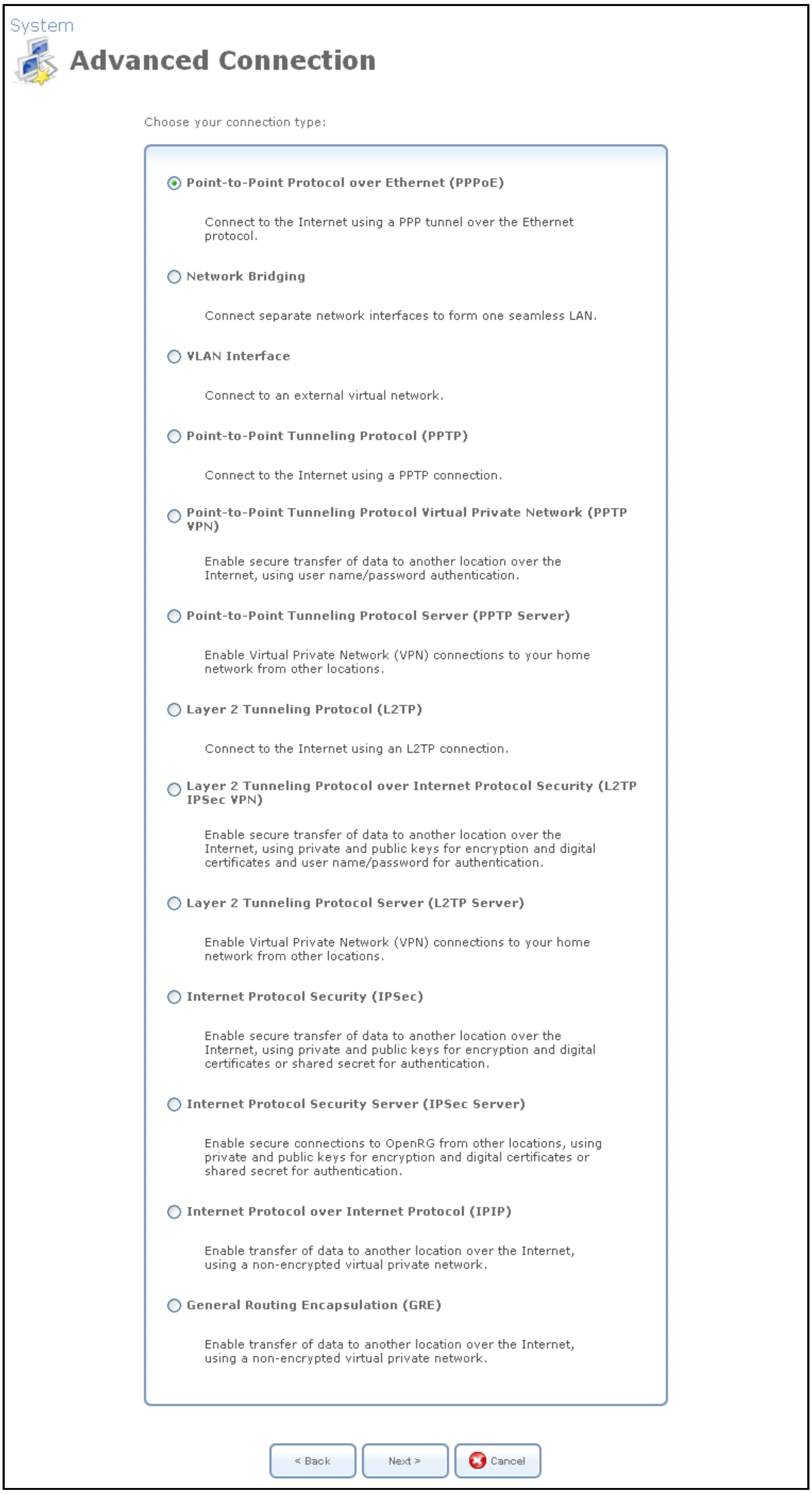


Figure 6.33 Advanced Connection Wizard

3. Select the 'Network Bridging' radio button and click 'Next'. The 'Bridge Options' screen appears.

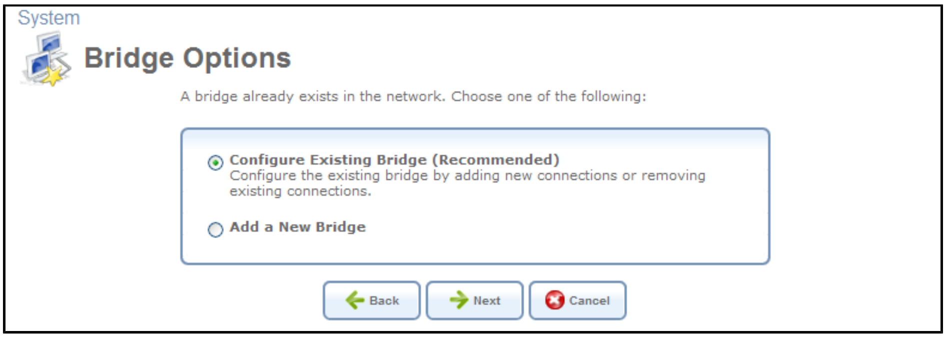


Figure 6.34 Bridge Options

4. Select whether to configure an existing bridge (this option will only appear if a bridge exists) or to add a new one:

   a. **Configure Existing Bridge** Select this option and click 'Next'. The 'Network Bridging' screen appears allowing you to add new connections to the bridge or remove existing ones, by selecting or deselecting their respective check boxes. For example, to create a WAN-LAN bridge, select the WAN connection's check box.

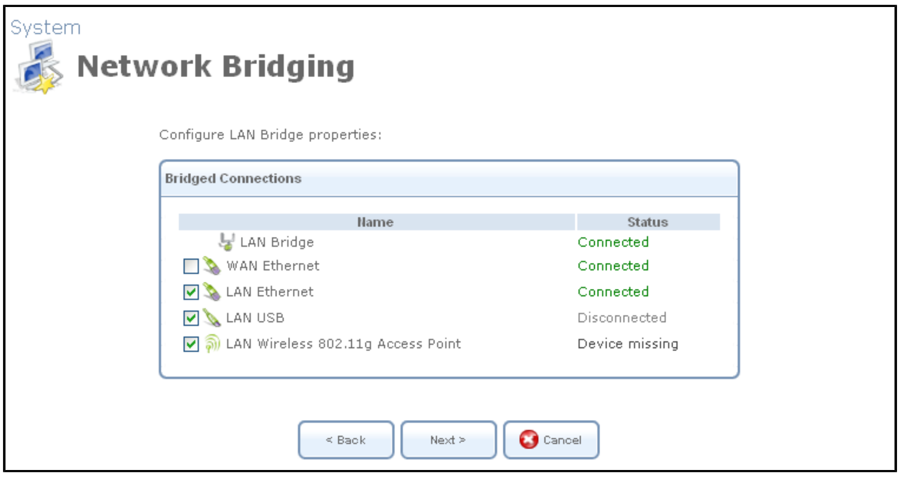


Figure 6.35 Network Bridging – Configure Existing Bridge

   b. **Add a New Bridge** Select this option and click 'Next'. A different 'Network Bridging' screen appears allowing you to add a bridge over the unbridged connections, by selecting their respective check boxes.

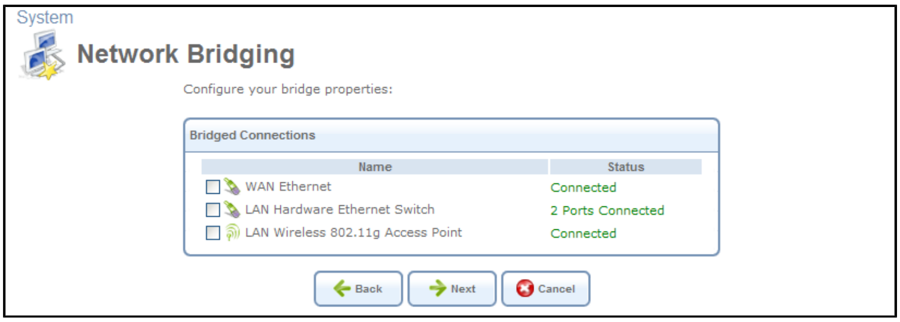


Figure 6.36 Network Bridging – Add a New Bridge

5. Click 'Next'. The 'Connection Summary' screen appears, corresponding to your changes.

Figure 6.37 Connection Summary – Configure Existing Bridge

6. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

7. Click 'Finish' to save the settings. The new bridge will be added to the network connections list, and it will be configurable like any other bridge.

The new bridge will be added to the network connections list, and it will be configurable like any other bridge.

Note: Creating a WAN-LAN bridge disables OpenRG's DHCP server. This means that LAN hosts may only receive an IP address from a DHCP server on the WAN. If you configure a host with a static IP address from an alias subnet of the bridge (192.168.1.X), you will be able to access OpenRG but not the WAN, as NAT is not performed in the WAN-LAN bridge mode.

6.4.5.2 Viewing and Editing the LAN Bridge Settings

After creating a bridge, you can view or modify its settings by clicking the bridge's entry in the 'Network Connections' screen. The 'LAN Bridge Properties' screen appears.

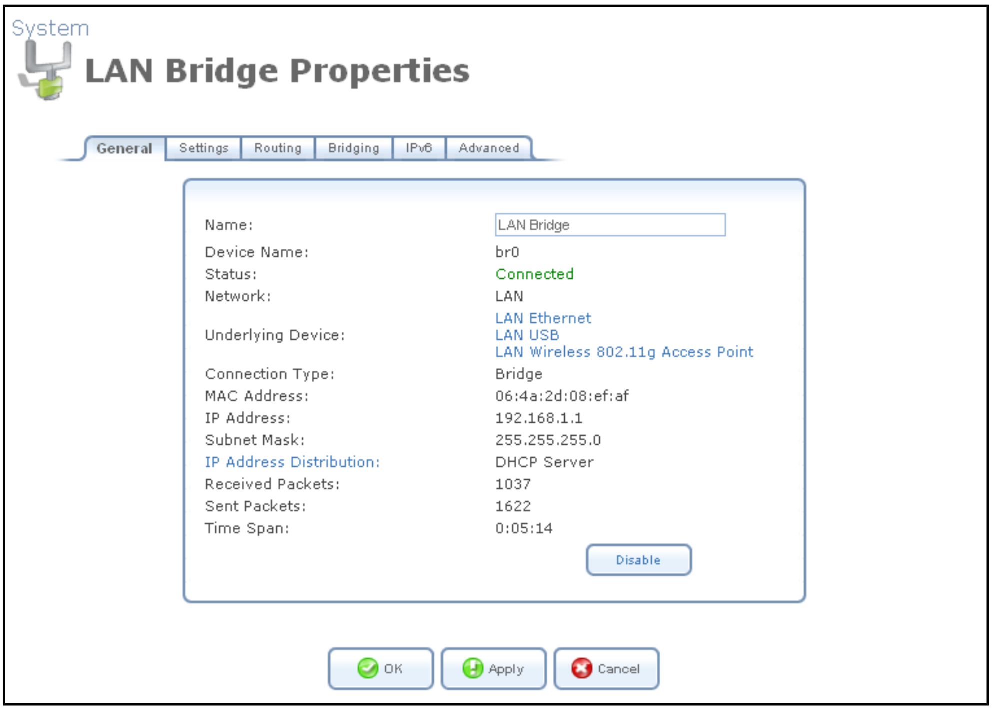


Figure 6.38 LAN Bridge Properties

6.4.5.2.1 General

This sub-tab enables you to view the LAN bridge connection settings (see Figure 6.38). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.5.2.2 Settings

This sub-tab enables you to edit the following LAN bridge settings.

General This section displays the connection's general parameters. It is recommended not to change the default values unless you are familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

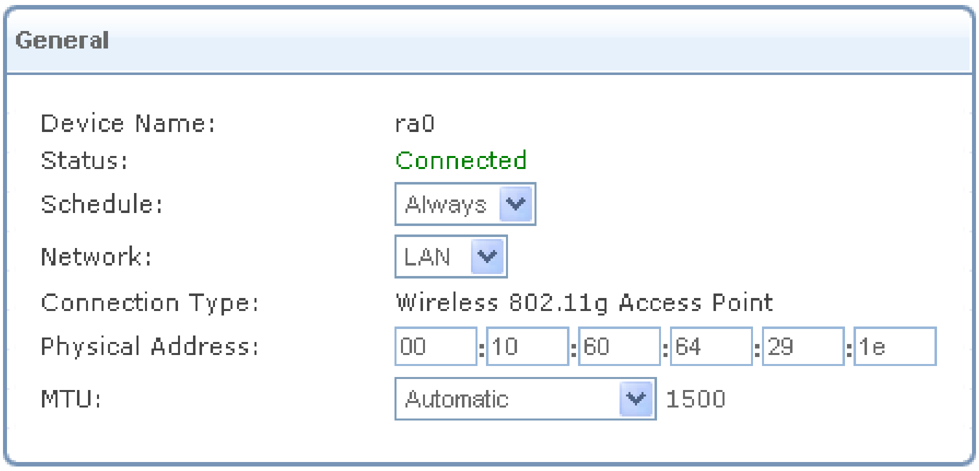


Figure 6.39 General Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen will refresh to display relevant configuration settings according to your choice.

No IP Address Select 'No IP Address' if you require that your gateway have no IP address. This can be useful if you are working in an environment where you are not connected to other networks, such as the Internet.

Figure 6.40 Internet Protocol – No IP Address

Obtain an IP Address Automatically Your connection is configured by default to act as a DHCP client. You should keep this configuration in case your service provider supports DHCP, or if you are connecting using a dynamic IP address. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask

instead. You can click the 'Release' button to release the current leased IP address. Once the address has been released, the button text changes to 'Renew'. Use the 'Renew' button to renew the leased IP address.

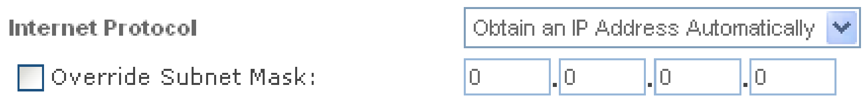


Figure 6.41 Internet Protocol Settings – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

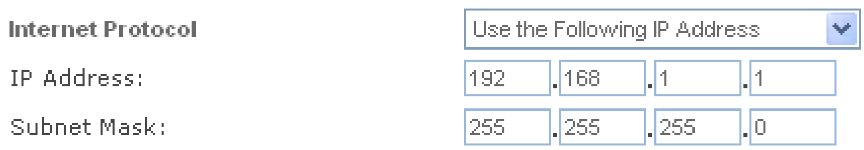


Figure 6.42 Internet Protocol – Static IP

DNS Server Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 6.43 DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

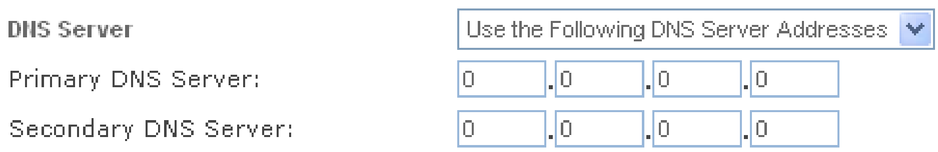


Figure 6.44 DNS Server – Static IP

To learn more about this feature, refer to Section 5.12.1.

IP Address Distribution The 'IP Address Distribution' section allows you to configure the gateway's Dynamic Host Configuration Protocol (DHCP) server parameters. The DHCP automatically assigns IP addresses to network PCs. If you enable this feature, make sure that you also configure your network PCs as DHCP clients. For a comprehensive description of this feature, refer to Section 5.11. Select one of the following options from the 'IP Address Distribution' drop-down menu:

- **DHCP Server**

In case you have chosen DHCP Server, complete the following fields:

Start IP Address The first IP address that may be assigned to a LAN host. Since the LAN interface's default IP address is 192.168.1.1, it is recommended that the first address assigned to a LAN host will be 192.168.1.2 or greater.

End IP Address The last IP address in the range that can be used to automatically assign IP addresses to LAN hosts.

Subnet Mask A mask used to determine to what subnet an IP address belongs. An example of a subnet mask value is 255.255.255.0.

Lease Time In Minutes Each device will be assigned an IP address by the DHCP server for this amount of time, when it connects to the network. When the lease expires the server will determine if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use will become available for other computers on the network.

Provide Host Name If Not Specified by Client If the DHCP client does not have a host name, the gateway will automatically assign one for it.

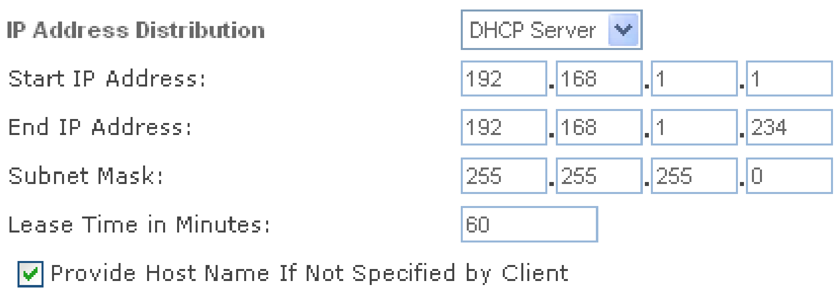


Figure 6.45 IP Address Distribution – DHCP Server

- **Disabled** Select 'Disabled' from the drop-down menu if you would like to statically assign IP addresses to your network computers.

Figure 6.46 IP Address Distribution – Disable DHCP

6.4.5.2.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

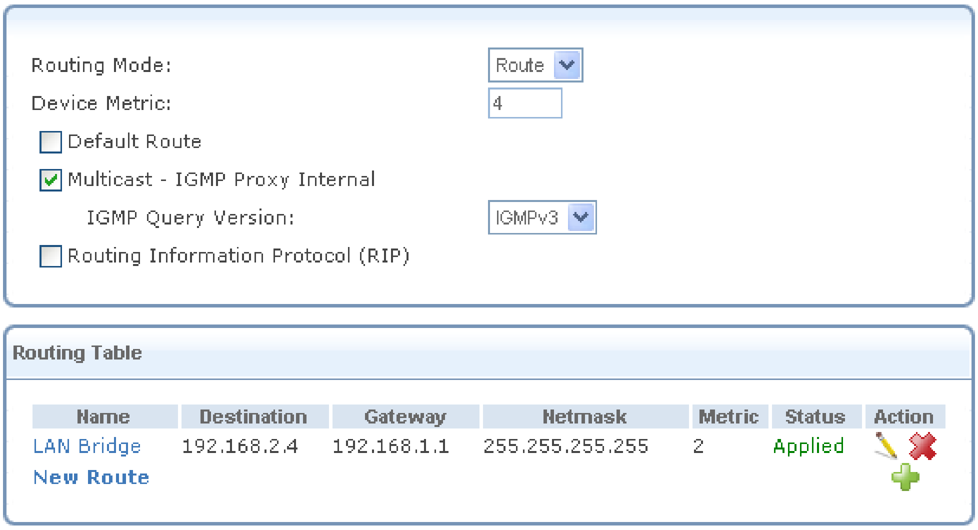


Figure 6.47 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

> **Route** Use route mode if you want your gateway to function as a router between two networks.
>
> **NAPT** Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

> **IGMP Query Version** OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
- **Send RIP messages**—select either 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.

Routing Table Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.
To learn more about this feature, refer to Section 6.6.

6.4.5.2.4 Bridging

This sub-tab enables you to specify the devices that you would like to join under the network bridge.

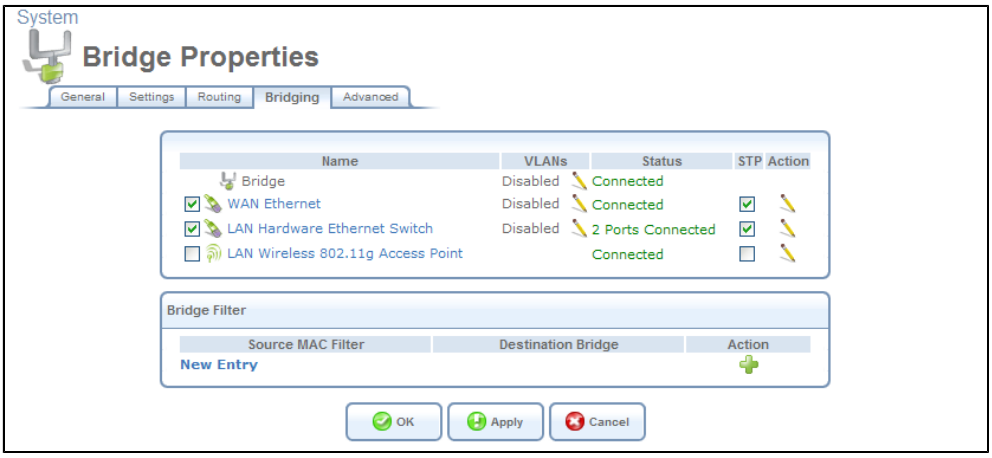


Figure 6.48 Bridge Settings

If you wish to assign the network connections to specific virtual LANS (VLANs), click the action icon under the 'VLANs' column.

Note: If you would like to logically partition your Ethernet-based network, you can set up a VLAN bridge as described in Section 6.4.16.4.

Select the 'STP' check box to enable the Spanning Tree Protocol on the device. Use this feature to ensure that there are no loops in your network configuration, especially in case your network consists of multiple switches, or other bridges apart from those created by the gateway. By blocking redundant connections, STP enables a single data path between LAN hosts. If a device or a link failure causes this path to become unusable, STP will enable an alternative path. Note that OpenRG also supports the Rapid Spanning Tree Protocol (RSTP), which provides a faster response to changes in your local network topology than STP.

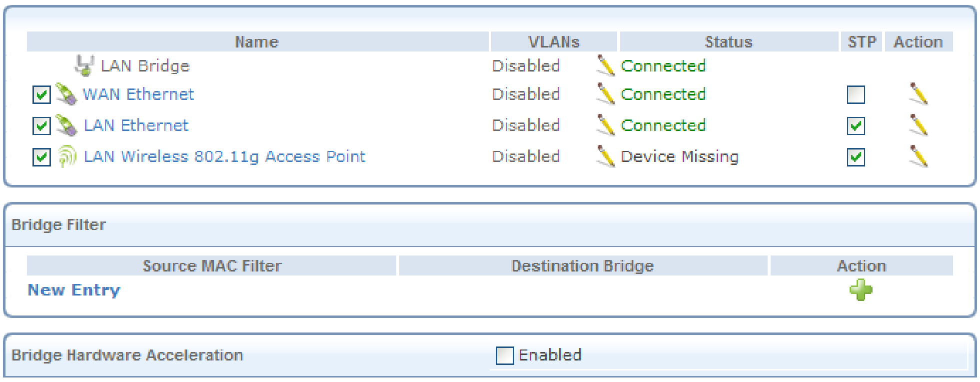


Figure 6.49 LAN Bridge Settings

Bridge Filter This section is used for creating a traffic filtering rule on the bridge, in order to enable direct packet flow between the WAN and the LAN. Such an example is when setting up a hybrid bridging mode (refer to Section 6.4.15.2).

Bridge Hardware Acceleration Select this check box to utilize the **Fastpath** algorithm for enhancing packet flow through the bridge. Note that this feature must be supported and enabled on the bridge's underlying devices in order to work properly.

6.4.5.2.5 IPv6

This subtab enables you to define new IPv6 addresses for the current connection, by clicking the 'New Unicast Address' link. Note that this sub-tab appears only if the IPv6 feature is enabled on the gateway. For more information, refer to Section 6.6.2.

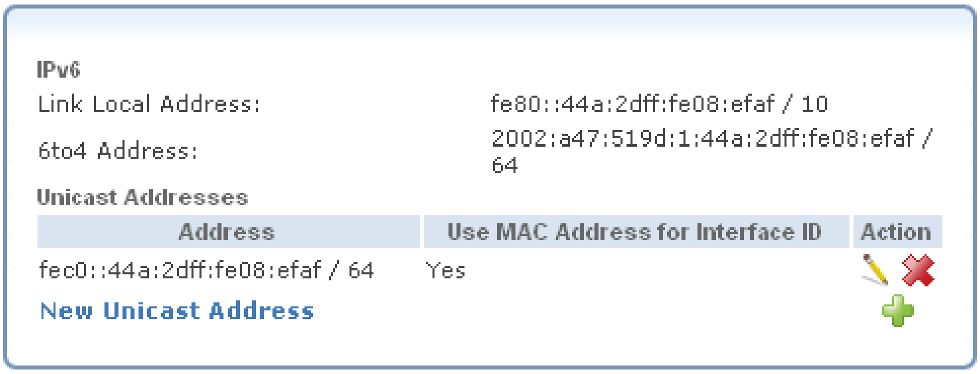


Figure 6.50 IPv6 Settings

6.4.5.2.6 Advanced

This sub-tab enables you to configure the advanced LAN bridge settings.

- **Internet Connection Firewall** Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

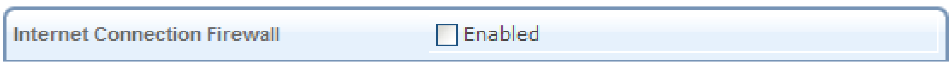


Figure 6.51 Internet Connection Firewall

- **Additional IP Addresses** You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://openrg.home.

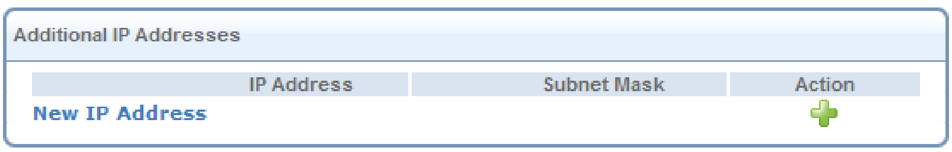


Figure 6.52 Additional IP Addresses

6.4.6 Setting Up a LAN Wireless Network

OpenRG provides broadband customer premise equipment (CPE) manufacturers with a complete software solution for developing feature-rich CPE with wireless connectivity over the 802.11 **b**, **g**, and **n** standards. The solution is vertically integrated and includes an operating system, communication protocols, routing, advanced wireless and broadband networking security, remote management and home networking applications.

OpenRG integrates multiple layers of wireless security. These include the IEEE 802.1x port-based authentication protocol, RADIUS client, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, Wi-Fi Protected Access (WPA), WPA2, WPA and WPA2 (mixed mode), as well as industry-leading OpenRG Firewall and VPN applications. In addition, OpenRG's built-in authentication server enables home/SOHO users to define authorized wireless users without the need for an external RADIUS server.

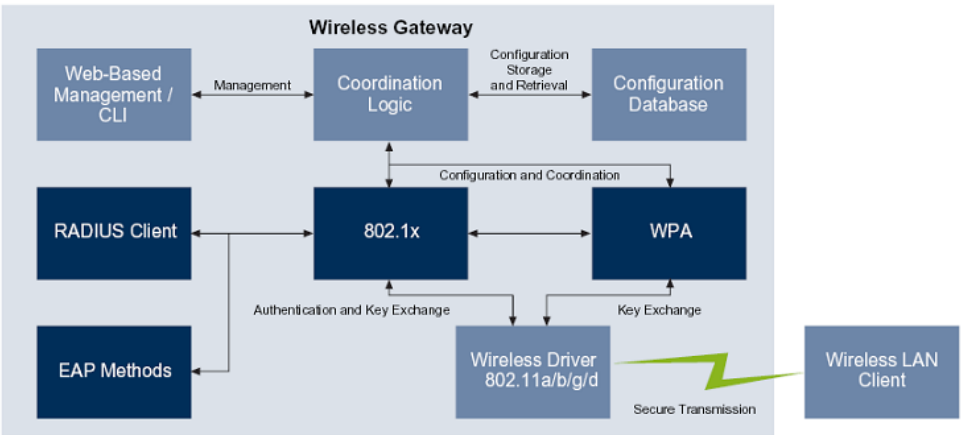


Figure 6.53 OpenRG for Wireless Gateways – Authentication and Encryption Components

6.4.6.1 Enabling OpenRG's Wireless Network Interface

To enable OpenRG's wireless network interface, perform the following:

1. Click the 'LAN Wireless 802.11g Access Point' link in the 'Network Connections' screen (see Figure 6.13). The 'LAN Wireless 802.11g Access Point Properties' screen appears.

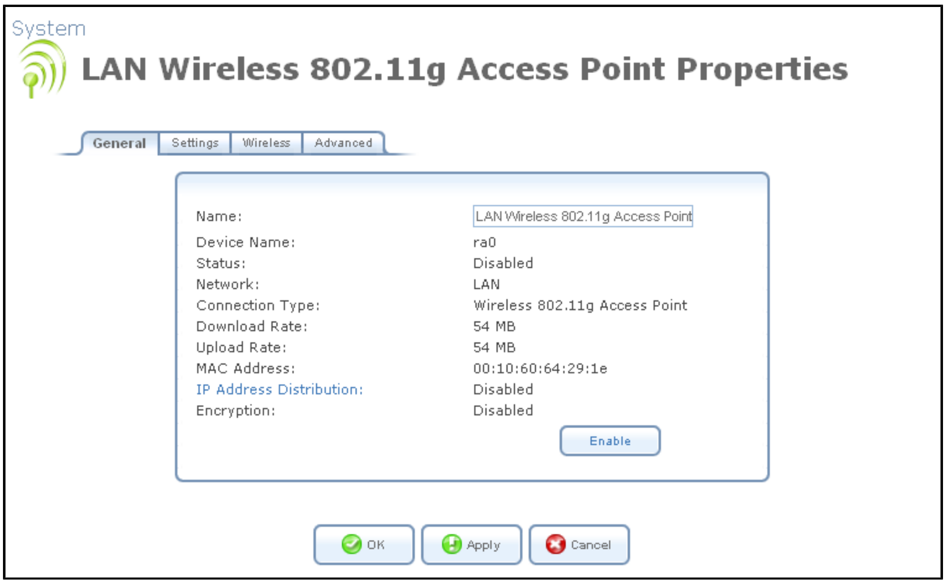


Figure 6.54 LAN Wireless 802.11g Access Point Properties – Disabled

2. Click the 'Enable' button (this button is displayed only if a wireless card is available on the gateway). The screen refreshes, and the connection status changes to "Connected".

3. Click the 'Wireless' sub-tab.

4. In the 'SSID' field, you may change the broadcasted name of your wireless network from the default to a more unique name.

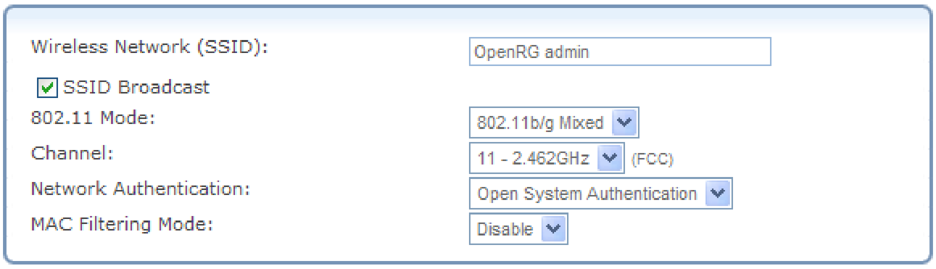


Figure 6.55 Wireless Access Point

5. Click 'OK' to save the settings.

Note: In order to connect a wireless PC to the gateway, you may also need to configure the PC, as described in the 'Connecting Your PC' section of the OpenRG User Manual.

By default, only HTTP authentication protects the wireless network from unauthorized users. Consider securing the wireless network using other methods as described in Section 6.4.6.4.

You can perform basic configuration of the gateway's wireless interface using the installation wizard, as described in Section 2.3. The following sections will familiarize you with OpenRG's wireless connection settings.

6.4.6.2 Passing Web Authentication

Prior to wireless authentication and encryption, the Web authentication feature protects your wireless network from unauthorized wireless clients. When wireless clients attempt to connect to OpenRG's WAN, they are prompted to enter a user name and password (see Figure 6.56). Note that all other attempts to use the wireless network prior to the authentication will fail (Telnet, FTP, ping).

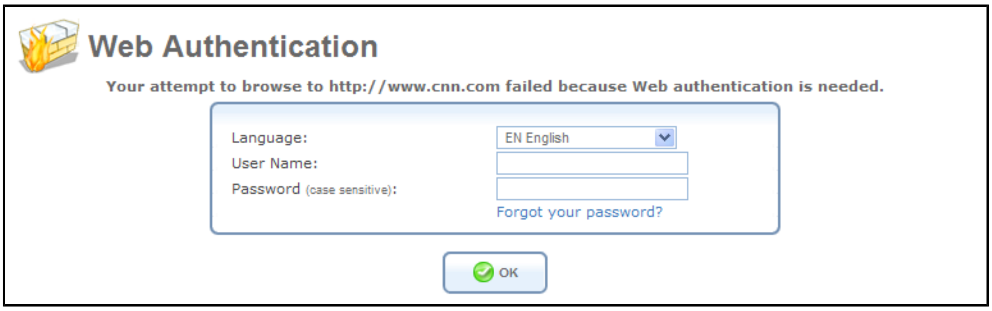


Figure 6.56 Web Authentication

As a wireless user, enter your user name and password and click 'OK'. Once authentication has been performed, you may proceed to use OpenRG's wireless network from the configured PC, for example to browse the Internet.

Figure 6.57 Web Authentication – Enabled Browsing

Note: Web authentication is available only after you first perform an initial configuration using the 'Quick Setup' screen and have an active WAN connection.

As the gateway's administrator, you can control the access that wireless users will have, via the WBM. In the 'Overview' screen under the 'Home' tab, you can allow or block wireless users in the 'Local Network' section, by clicking the respective links (the same section appears in the 'Overview' screen under the 'Local Network' tab).

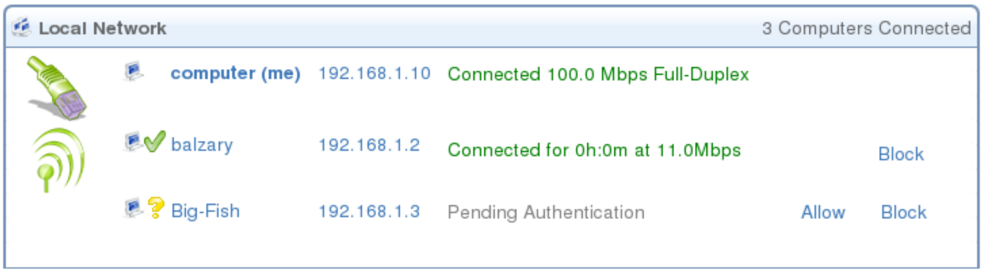


Figure 6.58 Home Overview – Local Network

Figure 6.58 depicts a connected wireless user (that can be blocked), and a user that has not been authenticated yet (hence, the yellow question mark appears). This user can be authenticated either by entering correct login details in the Web authentication screen, or by the gateway's administrator from this screen. Click 'Allow' to authenticate the user or 'Block' to reject. The screen will refresh and present the relevant action(s) that can be performed.

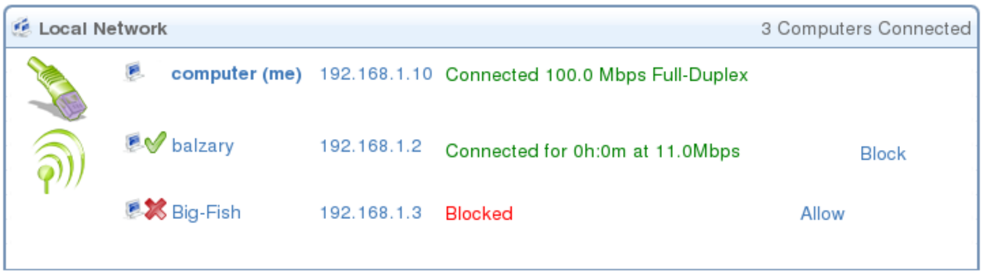


Figure 6.59 Home Overview – Local Network

6.4.6.3 Recovering Your Wireless Network's Password

When attempting to connect to the Internet via OpenRG's wireless access point, you are prompted to enter a username and password. In case you have forgotten your password, click the 'Forgot Your Password?' link that appears in the 'Web Authentication' screen (see Figure 6.56). The 'Forgotten Password for Wireless Network' screen appears, providing numerous possible courses of action aimed at helping you log in.

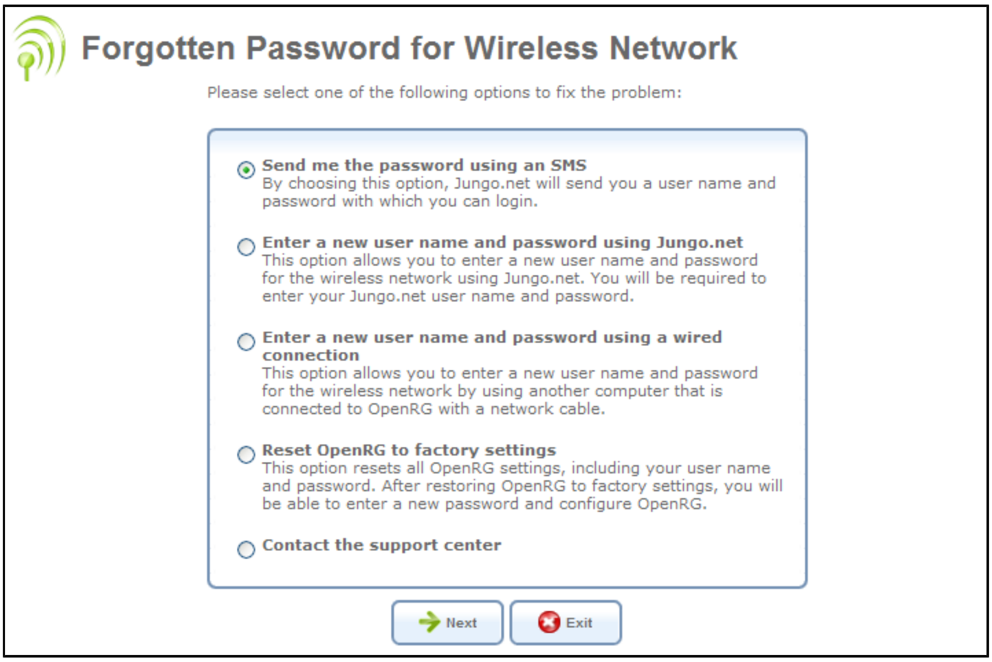


Figure 6.60 Forgotten Password for Wireless Network

Note: The first two options are displayed only if the gateway is connected to Jungo.net.

- **Send me the password by SMS** This option (selected by default) enables you to receive an SMS message containing your login details. To use this option, perform the following:

1. Verify that the feature's radio button is selected, and click 'Next'. The phone number prompt screen appears.

Figure 6.61 Cellphone Number Prompt

2. Enter your cellphone number in the format displayed in this screen, and click 'SMS Me!'. The following message appears.

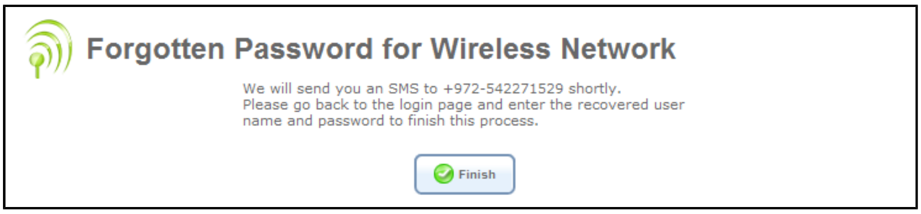


Figure 6.62 Sent SMS Confirmation

In a few moments, you will receive an SMS message containing your login details.

3. Click 'Finish'. The 'Web Authentication' screen appears (see Figure 6.56), enabling you to log in.

4. Enter your username and password, and click 'OK'. The following authentication message appears.

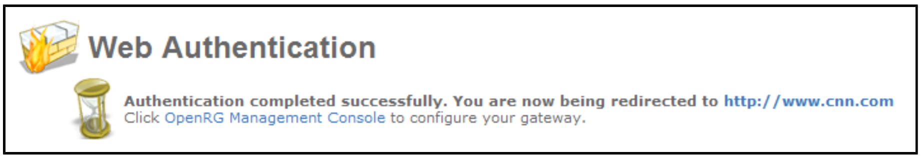


Figure 6.63 Successful Authentication

In a few moments, you will be redirected to the requested website.

- **Enter a new user name and password using Jungo.net** This option enables you to enter a new user name and password for the wireless network using Jungo.net.

1. To use this option, select its radio button and click 'Next'. The Jungo.net login screen appears.

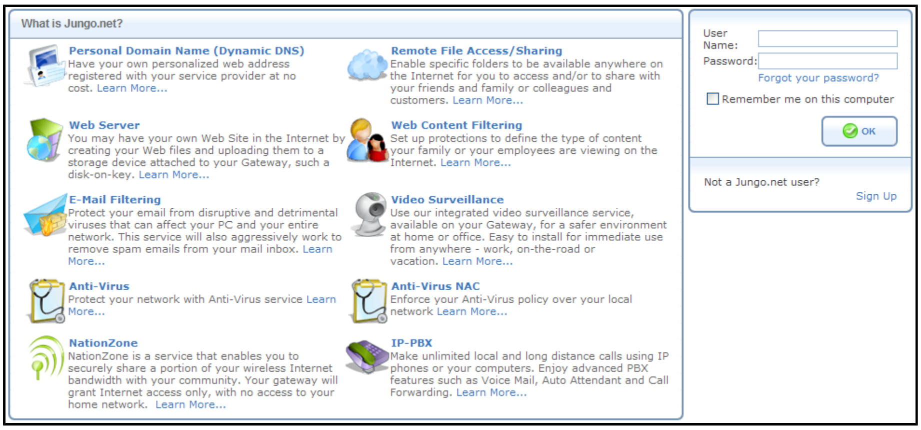


Figure 6.64 Jungo.net Login

2. Enter OpenRG's Jungo.net user name and password, and click 'OK'. The 'Wireless LAN User' screen appears.

Figure 6.65 Wireless LAN User

3. Create a new wireless client by entering a user name and password, and click 'Go'. The screen refreshes as the user is created, until the 'New User Created' screen appears.

Figure 6.66 New User Created

4. Click 'Finish'. OpenRG's login screen appears. You can now login with the new wireless client details.

- **Enter a new user name and password using a wired connection** This option allows you to enter a new user name and password for the wireless network by using another computer that is physically connected to OpenRG. To use this option, select its radio button and click 'Next'. The next screen contains a detailed description of the steps you must follow in order to create a new user name and password for the wireless network.

Figure 6.67 Enter a New User Name and Password Using a Wired Connection

- **Reset OpenRG to factory settings** This option resets OpenRG's settings, including your user name and password. To use this option, select its radio button and click 'Next'. The next screen contains a detailed description of the steps you must follow in order to reset OpenRG to its factory settings.

Figure 6.68 Reset Factory Settings

- **Contact the support center** If all previous methods have not been helpful, select this radio button and click 'Next'. The next screen contains instructions for calling the support center, and displays your gateway's identification required when opening a support call.

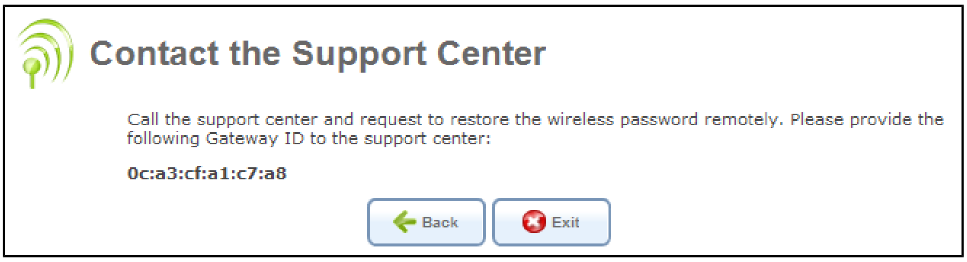


Figure 6.69 Contact the Support Center

6.4.6.4 Securing Your Wireless Network

OpenRG's wireless network is ready for operation with its default values. The following section describes how to secure your wireless connection using the **Wi-Fi Protected Access** (WPA) security protocol. The Wi-Fi Alliance created the WPA security protocol as a data encryption method for 802.11 wireless local area networks (WLANs). WPA is an industry-supported, pre-standard version of 802.11i utilizing the Temporal Key Integrity Protocol (TKIP), which fixes the problems of Wired Equivalent Privacy (WEP), including the use of dynamic keys.

6.4.6.4.1 Securing with WPA

To secure your wireless network with WPA, perform the following:

1. Click the 'LAN Wireless 802.11g Access Point' link in the 'Network Connections' screen. The 'LAN Wireless 802.11g Access Point Properties' screen appears:

Figure 6.70 LAN Wireless 802.11g Access Point Properties – Enabled

2. Click the 'Wireless' tab.

3. Enable the 'Wireless Security' feature by selecting its 'Enabled' check box. The screen will refresh, displaying the wireless security options (see Figure 6.71).

4. From the 'Stations Security Type' drop-down menu, select "WPA". Note that when selecting WPA, both WPA and WPA2 are supported.

5. Verify that the selected authentication method is "Pre-Shared Key".

6. In the 'Pre-Shared Key' text field, enter at least 8 characters. Verify that "ASCII" is selected in the associated drop-down menu.

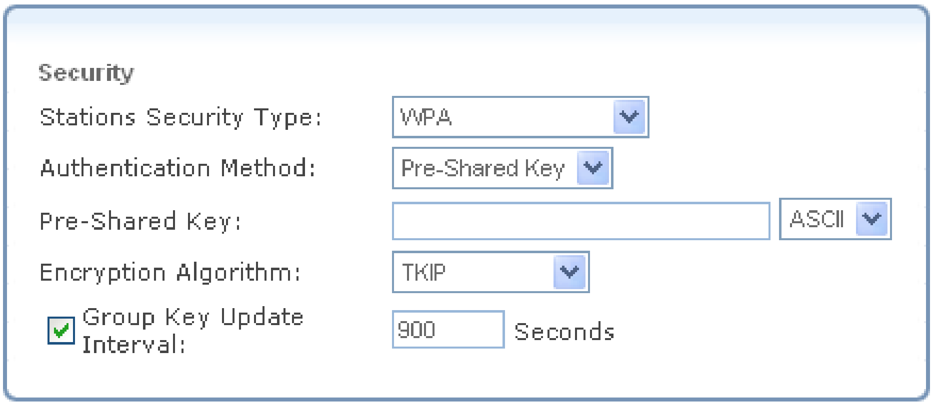


Figure 6.71 WPA Wireless Security Parameters

7. Click 'OK'. The following 'Attention' screen will appear warning you that OpenRG might require reloading.

Figure 6.72 Browser Reload Warning

8. Click 'OK' to save the settings.

6.4.6.4.2 Connecting a Wireless Windows Client

If your PC has wireless capabilities, Microsoft Windows™ will automatically recognize this and display a wireless connection icon in the system tray (alternatively, this icon is displayed in

the Windows 'Network Connections' screen, accessed from the Control Panel). Click this icon to search for and connect to your gateway's wireless network.

Alternatively, you can use the wireless client software supplied with your wireless hardware to connect to your wireless networks.

To manually establish a wireless connection between your PC and the gateway, perform the following:

1. Double-click the wireless connection icon that appears in the system tray. The 'Wireless Network Connection' screen appears, displaying OpenRG's wireless connection. Note that the connection is defined as "Security-enabled wireless network (WPA)".

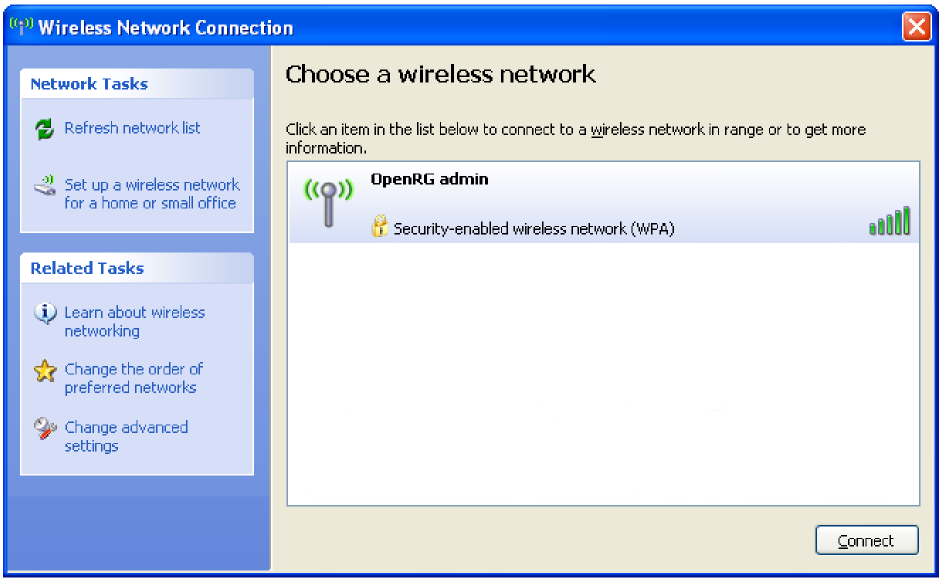


Figure 6.73 Available Wireless Connections

2. Click the connection once to mark it, and then click the 'Connect' button at the bottom of the screen. The following login window appears, asking for a 'Network Key', which is the pre-shared key you have configured.

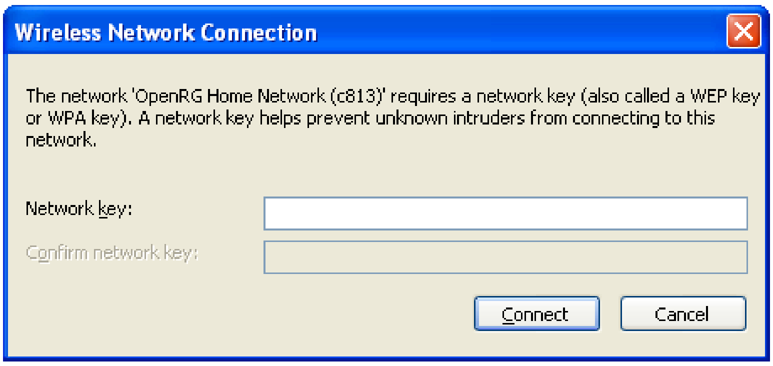


Figure 6.74 Wireless Network Connection Login

3. Enter the pre-shared key in both fields and click the 'Connect' button. After the connection is established, its status will change to 'Connected'.

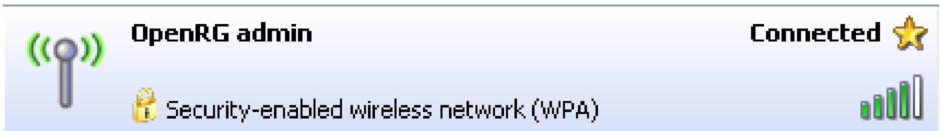


Figure 6.75 Connected Wireless Network

An icon will appear in the notification area, announcing the successful initiation of the wireless connection.

Figure 6.76 Wireless Connection Information

4. Test the connection by disconnecting all other networks and by browsing the Internet.

Should the login window above not appear and the connection attempt fail, configure the wireless connection manually:

1. Click the connection once to mark it, and then click the 'Change advanced settings' link in the 'Related Tasks' box on the left part of the window (see Figure 6.73). The 'Wireless Network Connection Properties' window appears.

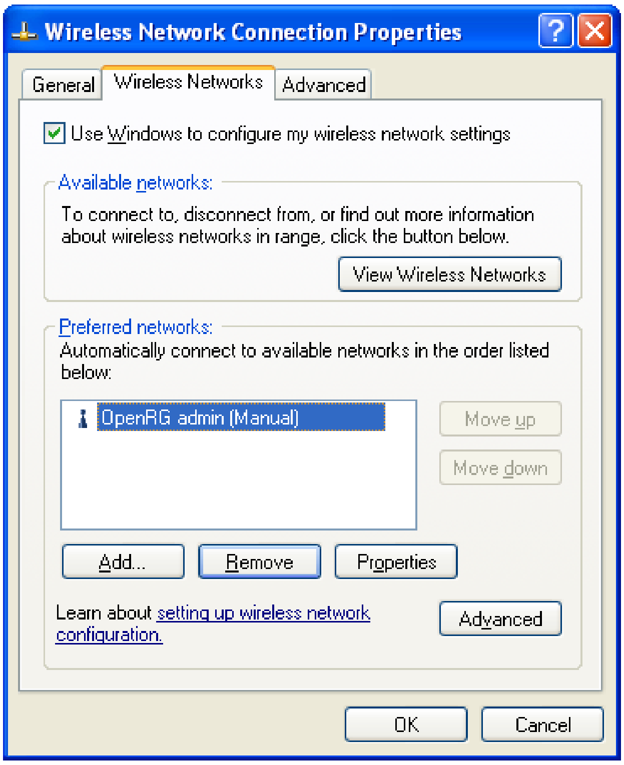


Figure 6.77 Wireless Network Connection Properties

2. Select the 'Wireless Networks' tab (see Figure 6.77).

3. Click your connection to highlight it, and click the 'Properties' button. Your connection's properties window appears.

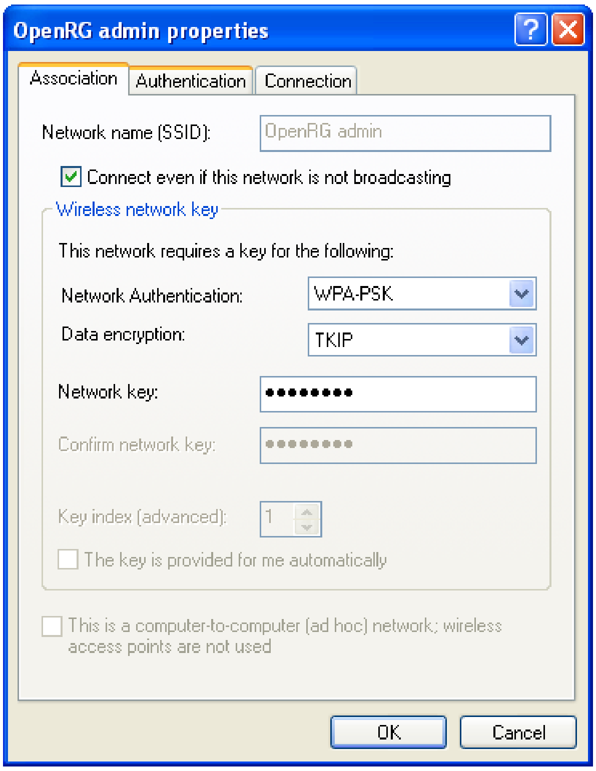


Figure 6.78 Connection Properties Configuration

a. From the 'Network Authentication' drop-down menu, select "WPA-PSK".

b. From the 'Data Encryption' drop-down menu, select "TKIP".

c. Enter your pre-shared key in both the 'Network key' and the 'Confirm network key' fields.

4. Click 'OK' in both windows to save the settings.

5. When attempting to connect to the wireless network, the login window will appear, pre-filled with the pre-shared key. Click the 'Connect' button to connect.

Since your network is now secured, only users that know the pre-shared key will be able to connect. The WPA security protocol is similar to securing network access using a password. Note that when selecting WPA, both WPA and WPA2 are supported.

6.4.6.5 Configuring General Wireless Parameters

The 'LAN Wireless 802.11g Access Point Properties' screen displays a detailed summary of the wireless connection's parameters, under the 'General' sub-tab.

Figure 6.79 LAN Wireless 802.11g Access Point Properties – Enabled

Use the 'Settings' sub-tab to edit these parameters.

General This section displays the connection's general parameters. It is recommended not to change the default values unless you are familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

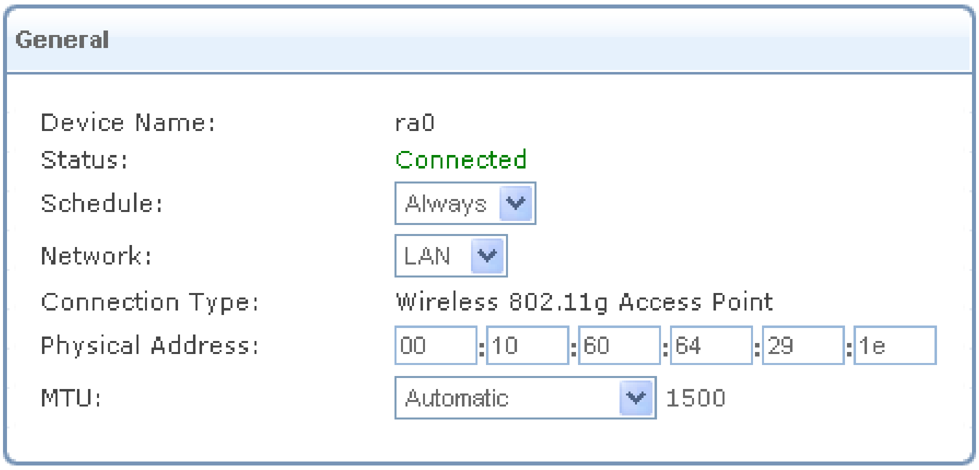


Figure 6.80 General Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more

information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

6.4.6.6 Defining Advanced Wireless Access Point Settings

The 'Wireless' and 'Advanced' sub-tabs enable you to perform advanced configuration of your wireless access point.

6.4.6.6.1 Wireless Network

Use this section to define the basic wireless access point settings.

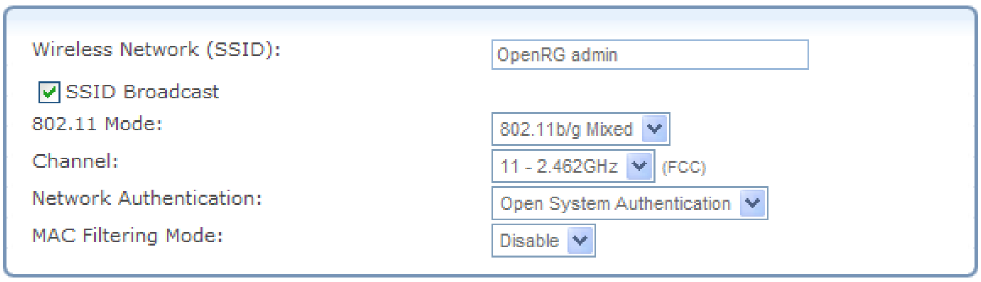


Figure 6.81 Wireless Access Point

SSID Broadcast By default, OpenRG broadcasts the name of its wireless network (SSID). For security reasons, you may choose to hide your wireless network by deselecting this check box. Wireless clients will only be able to connect by manually typing the SSID in their wireless client applications (whether Windows or a third party application), rather than choosing it from the list of available wireless networks.

802.11 Mode The modes available in this drop-down menu are the wireless communication standards supported by your gateway's wireless card. Select the 802.11 mode that is compatible with your network's wireless clients. Only clients of this mode will be able to communicate

with the gateway. Note that 802.11b legacy devices are not compatible with modes 802.11g/n and 802.11g Only.

Channel All devices in your wireless network must broadcast on different channels in order to function correctly. It is best to leave this parameter on Automatic. This ensures that OpenRG continuously scans for the most available wireless channel in the vicinity. It is possible to select a channel manually if you have information regarding the wireless channels used in your vicinity. The channels available depend on the regulatory authority (stated in brackets) to which your gateway conforms. For example, the European regulatory authority (ETSI) has allocated 13 available channels, while the US regulatory authority (FCC) has allocated 11 available channels.

Channel Width Mode This option appears on platforms supporting 802.11n only. Select the MHz width of the wireless channel, depending on your selected communication standard. For b and g, select either "20 MHz only" or "20/40 MHz (dynamic)". For 802.11n any mode may be selected.

Network Authentication The WPA network authentication method is 'Open System Authentication', meaning that a network key is not used for authentication. When using the 802.1X WEP or Non-802.1X WEP security protocols, this field changes to a drop-down menu, offering the 'Shared Key Authentication' method (which uses a network key for authentication), or both methods combined.

MAC Filtering Mode You can filter wireless users according to their MAC address, either allowing or denying access. Choose the action to be performed by selecting it from the drop-down menu.

6.4.6.6.2 MAC Filtering Table

Use this section to define advanced wireless access point settings. Click 'New MAC Address' to define filtering of MAC addresses. The 'MAC Filtering Settings' screen appears.

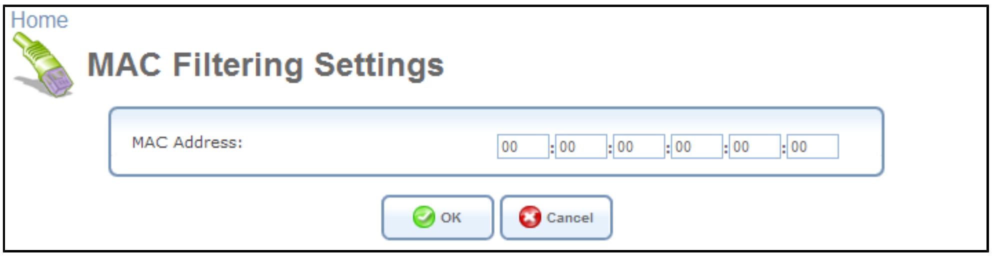


Figure 6.82 MAC Filtering Settings

Enter the MAC address to be filtered and click 'OK' button. A MAC address list appears, upon which the selected filtering action (allow/deny) will be performed.

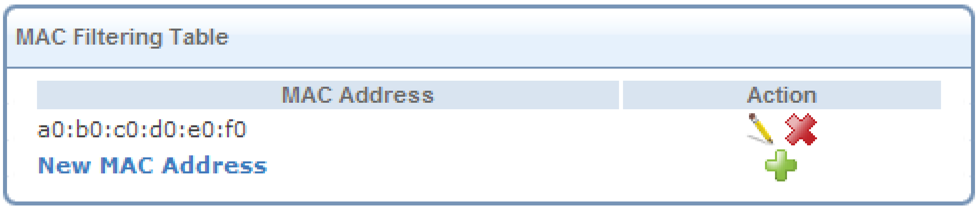


Figure 6.83 MAC Filtering Table

6.4.6.6.3 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is a method for simplifying the security setup and management of wireless networks. This feature is available on OpenRG, but is disabled by default. By enabling it, you can control the setup of your wireless security, which is defined in the following 'Security' section of the screen (refer to Section 6.4.6.6.4). Note that WPS only supports the WPA security protocol, therefore when enabling this feature, all other types of protocols are disabled (and are no longer available in the 'Security' section drop-down menu).

To enable WPS, click the 'Enabled' check box. The screen refreshes.

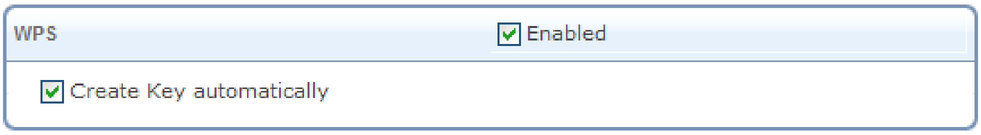


Figure 6.84 Wi-Fi Protected Setup

Create Key automatically You can either enter a security key manually, or have it generated automatically. Select your preference using the provided check box, and click 'Apply'. The screen refreshes.

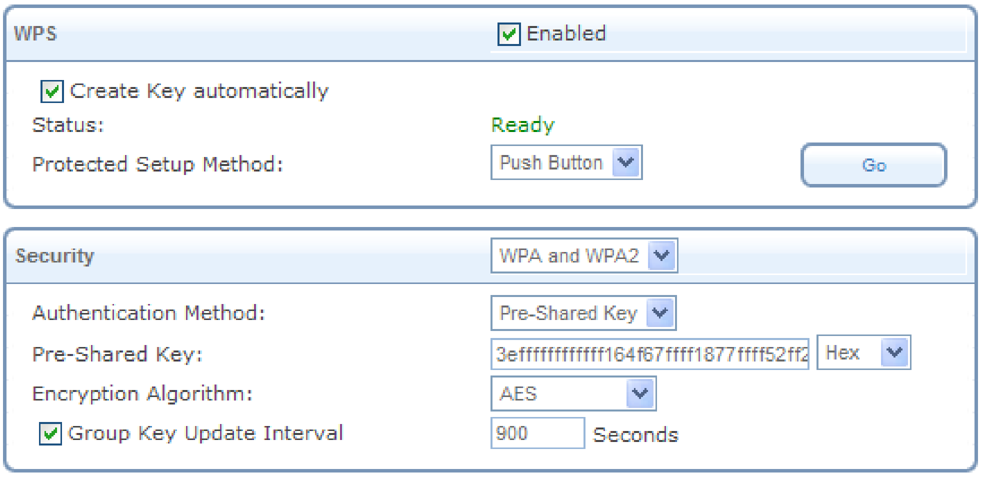


Figure 6.85 Enabled WPS

If you had chosen automatic key generation, a pre-shared key (of hexadecimal value) has been generated, and appears in the 'Security' section. You can enter/change the value at anytime by typing a different one in the field, as well as change the type of the value to ASCII using the provided drop-down menu.

Status Indicates the WPS status. "Ready" means that the system is ready to negotiate with incoming wireless clients, or "enrollees".

Protected Setup Method OpenRG supports two setup methods, "Push Button" (the default) and "Pin Code". These are the methods used by wireless clients when seeking an access point.

- **Push Button** – The enrollment is initiated by either pressing a physical button on the wireless client or through its software. After initiating the enrollment, click 'Go' for the devices to establish a connection.

- **Pin Code** – The enrollment is initiated by the wireless client's software, which also provides a pin code. To comply with this method, select this option from the drop-down menu. The screen refreshes to provide a field for entering the pin code:

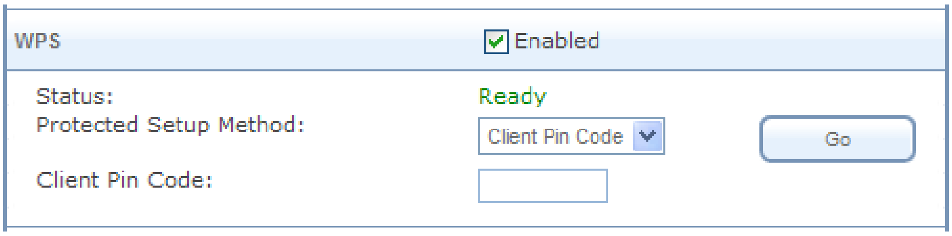


Figure 6.86 Protected Setup Method – Pin Code

In this field, enter the eight digit pin code provided by the wireless client's software. Click 'Go' for the devices to establish a connection.

When attempting to connect a wireless client to OpenRG, you must be aware of its setup method. A connection attempt will time out after two minutes if no connection is established. If a connection is established, the 'Status' field will change to reflect that.

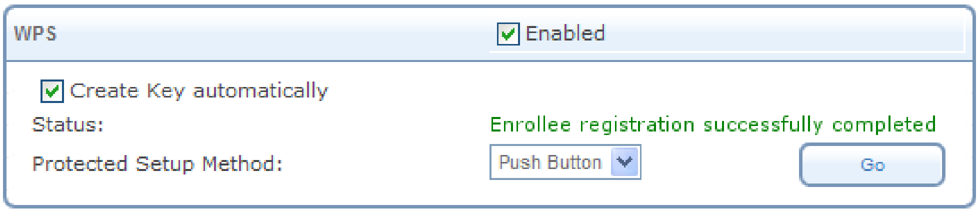


Figure 6.87 Successful Enrollee Registration

6.4.6.6.4 Security

Use this section to configure your wireless security settings. Select the type of security protocol in the 'Stations Security Type' drop-down menu. The screen refreshes, presenting each protocol's configuration respectively.

- **None** Selecting this option disables security on your wireless connection.

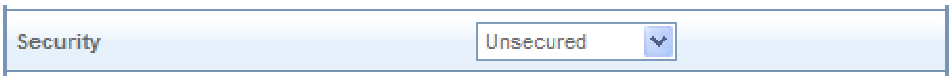


Figure 6.88 Disabled Wireless Security

- **WPA** WPA is a data encryption method for 802.11 wireless LANs (refer to Section 6.4.6.4).

  Authentication Method Select the authentication method you would like to use. You can choose between Pre-Shared Key and 802.1x.

  Pre-Shared Key This entry appears only if you had selected this authentication method. Enter your encryption key in the 'Pre-Shared Key' field. You can use either an ASCII or a Hex value by selecting the value type in the drop-down menu provided.

  Encryption Algorithm Select between Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) for the encryption algorithm.

Group Key Update Interval Defines the time interval in seconds for updating a group key.

Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

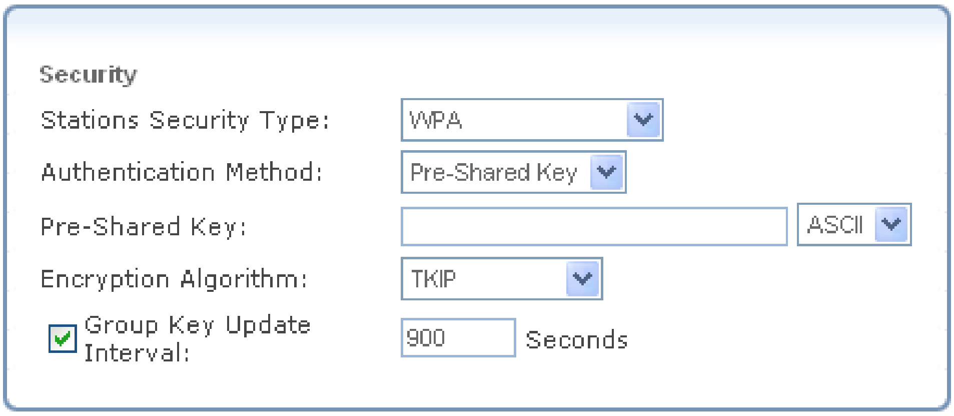


Figure 6.89 WPA Wireless Security Parameters

- **WPA2** WPA2 is an enhanced version of WPA, and defines the 802.11i protocol.

Authentication Method Select the authentication method you would like to use. You can choose between Pre-Shared Key and 802.1x.

Pre-Shared Key This entry appears only if you had selected this authentication method. Enter your encryption key in the 'Pre-Shared Key' field. You can use either an ASCII or a Hex value by selecting the value type in the drop-down menu provided.

Pre Authentication When selecting the 802.1x authentication method, these two entries appear (see Figure 6.90). Select this option to enable OpenRG to accept RADIUS authentication requests from computers connected to other access points. This enables roaming from one wireless network to another.

PMK Cache Period The number of minutes before deletion (and renewal) of the Pairwise Master Key used for authentication.

Figure 6.90 802.1x Authentication Method

Encryption Algorithm The encryption algorithm used for WPA2 is the Advanced Encryption Standard (AES).

Group Key Update Interval Defines the time interval in seconds for updating a group key.

Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

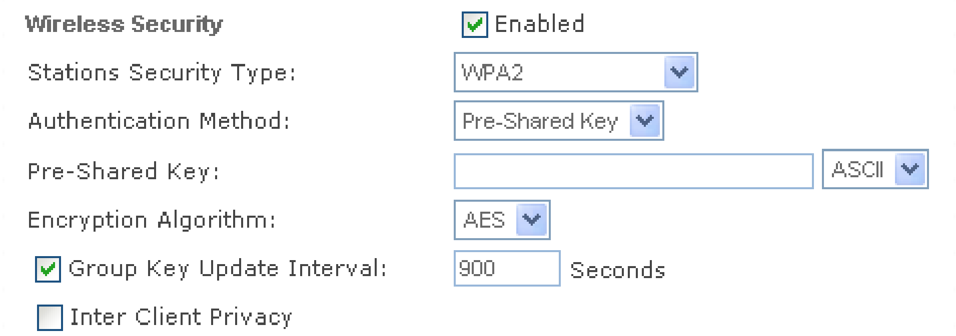


Figure 6.91 WPA2 Wireless Security Parameters

- **WPA and WPA2 Mixed Mode** WPA and WPA2 is a mixed data encryption method.

Authentication Method Select the authentication method you would like to use. You can choose between Pre-Shared Key and 802.1x.

Pre-Shared Key This entry appears only if you had selected this authentication method. Enter your encryption key in the 'Pre-Shared Key' field. You can use either an ASCII or a Hex value by selecting the value type in the drop-down menu provided.

Pre Authentication When selecting the 802.1x authentication method, these two entries appear (see Figure 6.92). Select this option to enable OpenRG to accept RADIUS authentication requests from computers connected to other access points. This enables roaming from one wireless network to another.

PMK Cache Period The number of minutes before deletion (and renewal) of the Pairwise Master Key used for authentication.

Figure 6.92 802.1x Authentication Method

Encryption Algorithm The encryption algorithm used for WPA and WPA2 is a either the Temporal Key Integrity Protocol (TKIP) or the Advanced Encryption Standard (AES).

Group Key Update Interval Defines the time interval in seconds for updating a group key.

Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

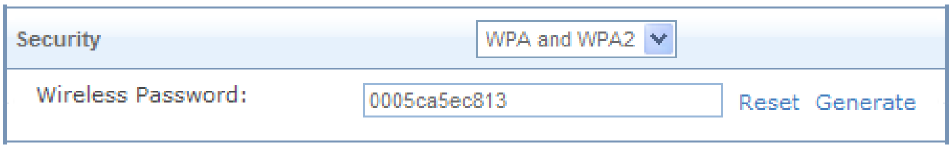


Figure 6.93 WPA and WPA2 Wireless Security Parameters

- **802.1x WEP** 802.1x WEP is a data encryption method utilizing an automatically defined key for wireless clients that use 802.1x for authentication and WEP for encryption.

  Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

  RADIUS Server Configure the RADIUS Server parameters (for more information, refer to Section 5.12.3).

  - **Server IP** Enter the RADIUS server's IP address.
  - **Server Port** Enter the RADIUS server's port.
  - **Shared Secret** Enter your shared secret.

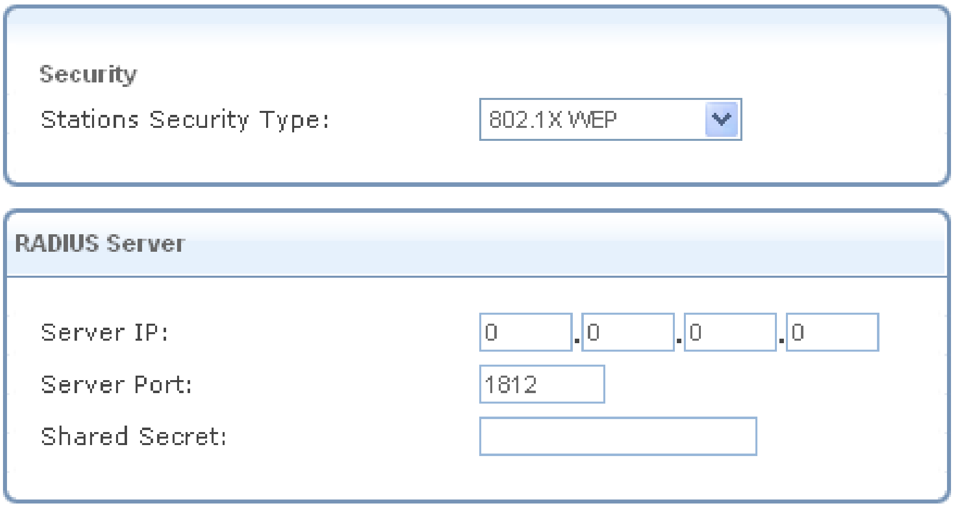


Figure 6.94 802.1x WEP Wireless Security Parameters

- **Non-802.1x WEP** Non-802.1x WEP is a data encryption method utilizing a statically defined key for wireless clients that do not use 802.1x for authentication, but use WEP for encryption. You may define up to four keys but use only one at a time. Note that the static key must be defined in the wireless Windows client as well.

  Inter Client Privacy Select the check box to prevent communication between the wireless network clients using the same access point. Clients will not be able to view and access each other's shared directories.

  Active Select the encryption key to be activated.

Encryption Key Type the encryption key until the entire field is filled. The key cannot be shorter than the field's length.

Entry Method Select the character type for the key: ASCII or HEX.

Key Length Select the key length in bits: 40 or 104 bits.

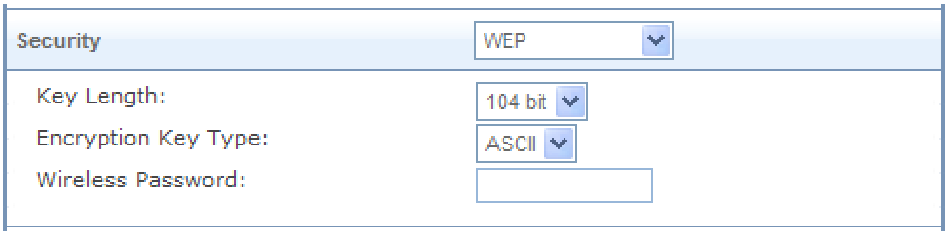


Figure 6.95 Non-802.1x WEP Wireless Security Parameters

The encryption key must be defined in the wireless Windows client as well. This is done in the Connection Properties Configuration window (to learn how to reach this window, refer to Section 6.4.6.4.2 [356]).

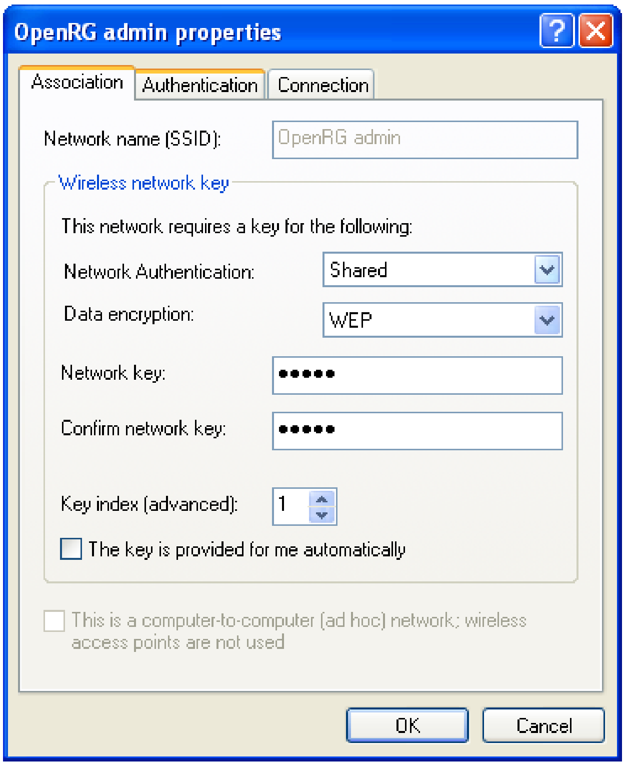


Figure 6.96 Connection Properties Configuration

1. In the 'Network Authentication' drop-down menu, select "Shared".

2. In the 'Data Encryption' drop-down menu, select "WEP".

3. Enter your encryption key in both the 'Network key' and the 'Confirm network key' fields.

- **Authentication Only** When selecting this option, wireless clients attempting to connect to the wireless connection will receive OpenRG's main login screen, along with the following attention message:

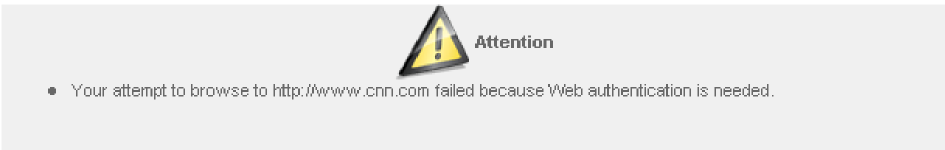


Figure 6.97 Web Authentication Needed

By logging into the WBM, clients authenticate themselves and are then able to use the connection. OpenRG keeps record of authenticated clients. To clear this list, click the 'Clean Mac List' button. Clients will have to re-authenticate themselves in order to use the wireless connection.

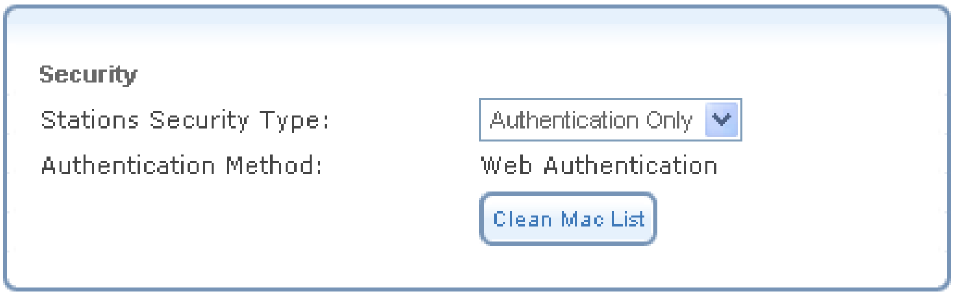


Figure 6.98 Authentication Only Wireless Security Parameters

6.4.6.6.5 Wireless WDS

OpenRG supports Wireless Distribution System (WDS), which enables wireless bridging of access points within its range. Virtual access points are used to interact with OpenRG's WDS peers, granting LAN users access to remote wireless networks.

> Note: Different wireless cards support a different number of virtual access points. The scenarios depicted herein refer to the **Ralink RT-2561** wireless card, supporting up to four virtual wireless access points.

Select the 'Enabled' check-box. The screen refreshes.

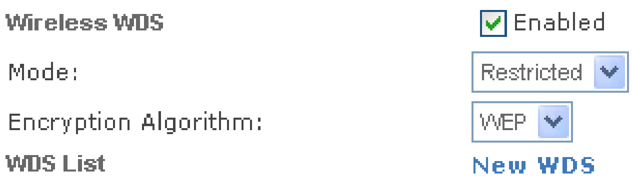


Figure 6.99 Wireless WDS

Mode OpenRG's WDS can function in one of the following modes:

- **Restricted –** WDS peers must be registered with OpenRG (by MAC addresses).

- **Bridge** – OpenRG will function as a wireless bridge, merely forwarding traffic between access points, and will not respond to wireless requests. The WDS peers must be manually stated and wireless stations will not be able to connect to OpenRG.
- **Repeater** – OpenRG will act as a repeater, interconnecting between access points. WDS peers can be determined by the user ('Restricted' mode) or auto-detected ('Lazy' mode).
- **Lazy** – Automatic detection of WDS peers: when a LAN user searches for a network, OpenRG will attempt to connect to WDS devices in its vicinity.

Encryption Algorithm When wireless security is enabled (refer to Section 6.4.6.6.4), this drop-down menu will display the encryption algorithms available for encrypting the communication between access points.

To add a WDS device, perform the following:

1. Click the 'New WDS' link, and then the 'Apply' button. If an 'Attention' screen appears, click 'OK'. The screen refreshes (see Figure 6.100), and a new virtual device appears in the WDS list, with the initial status of disabled.

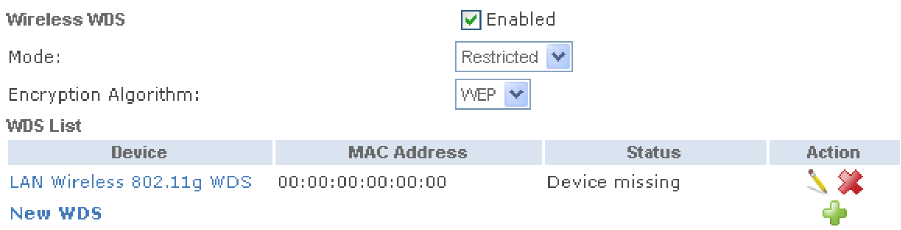


Figure 6.100 Wireless WDS – New WDS

Note that devices added to the WDS list before the WDS feature is enabled in the main device appears as missing.

2. Click the new device's action icon . The 'LAN Wireless 802.11g WDS Properties' screen appears (see Figure 6.101).

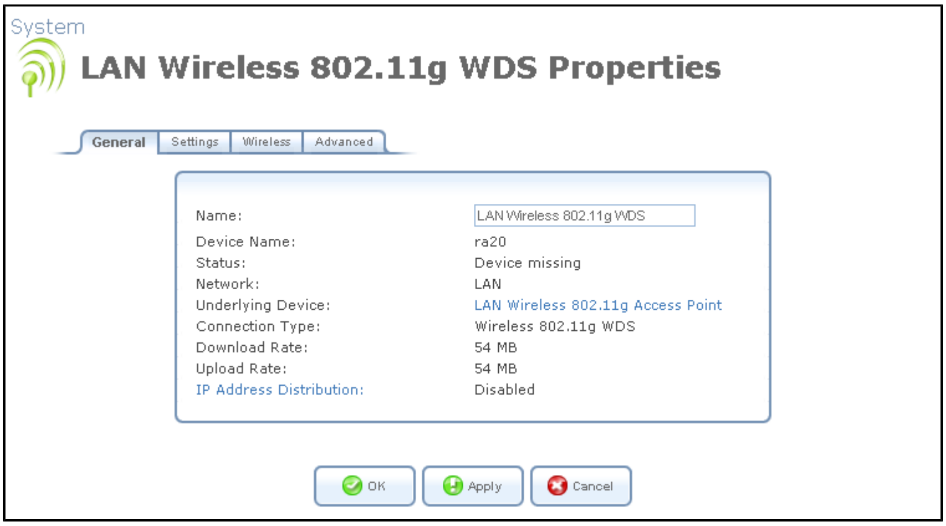


Figure 6.101 LAN Wireless 802.11g WDS Properties

3. Click the Wireless tab, and enter the MAC address of the WDS peer with which this virtual access point is to interact, in the 'Other AP' section.

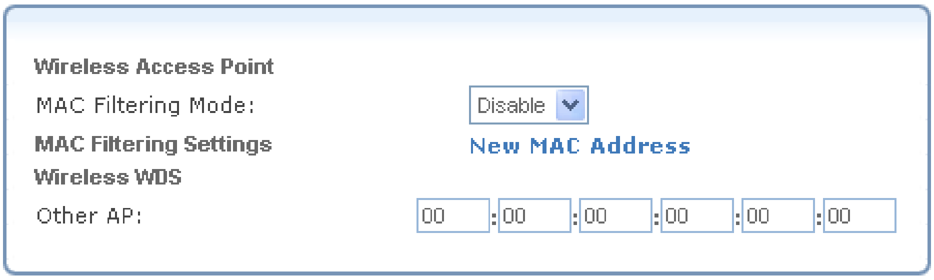


Figure 6.102 LAN Wireless 802.11g WDS Properties – Wireless Tab

4. Click 'OK'. The 'Network Connections' screen appears, displaying the new virtual 'LAN Wireless 802.11g WDS' connection.

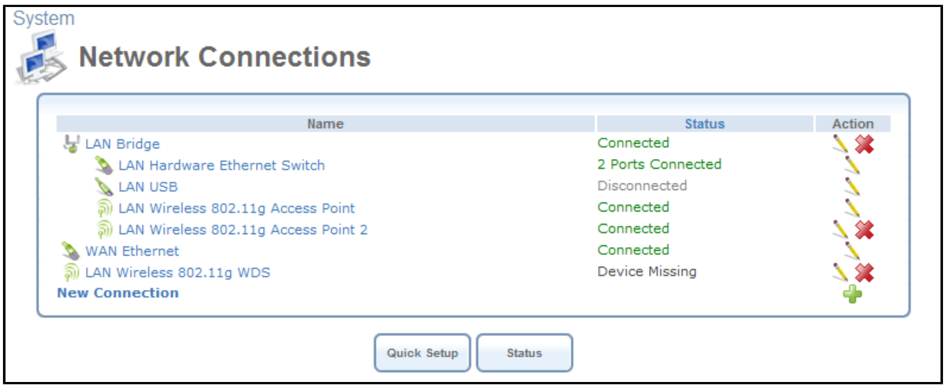


Figure 6.103 Network Connections

5. Click the virtual connection's  action icon . The 'LAN Wireless 802.11g WDS Properties' screen reappears.

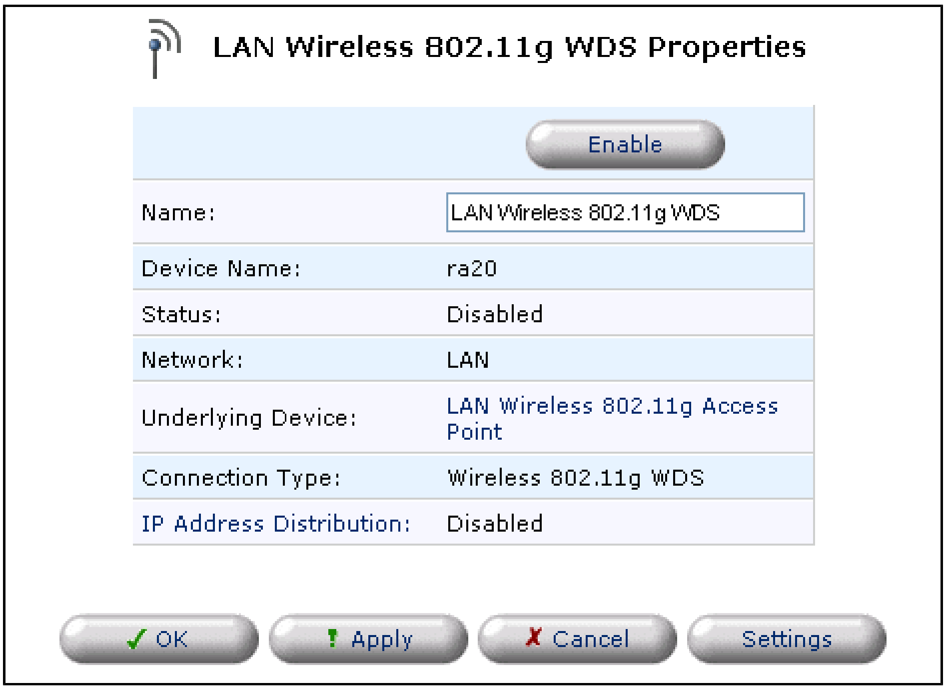


Figure 6.104 LAN Wireless 802.11g WDS Properties

6. Click the 'Enable' button. The virtual connection is now enabled. Go back to the physical wireless connection configuration screen to view its details.

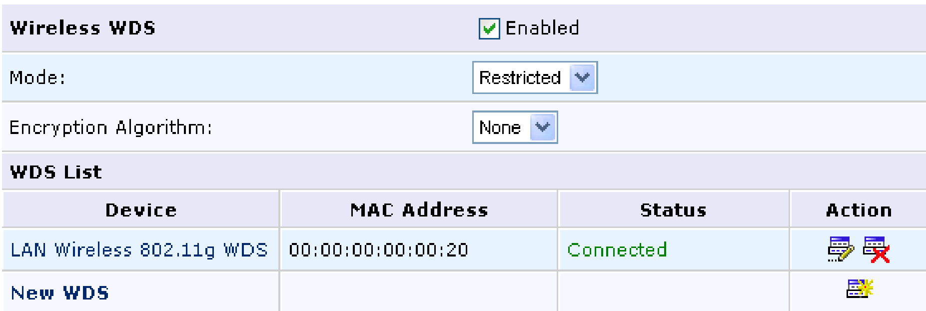


Figure 6.105 Wireless WDS

If the WDS peer also operates in 'Restricted' mode, it should similarly be configured with OpenRG's MAC address in order for both access points to communicate.

6.4.6.6.6 Wireless QoS (WMM)

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance certification, based on the IEEE 802.11e draft standard. It provides basic Quality of Service (QoS) features to IEEE 802.11 networks. If your gateway's wireless card supports WMM, you can enable this feature by checking its 'Enabled' check box. The screen refreshes.

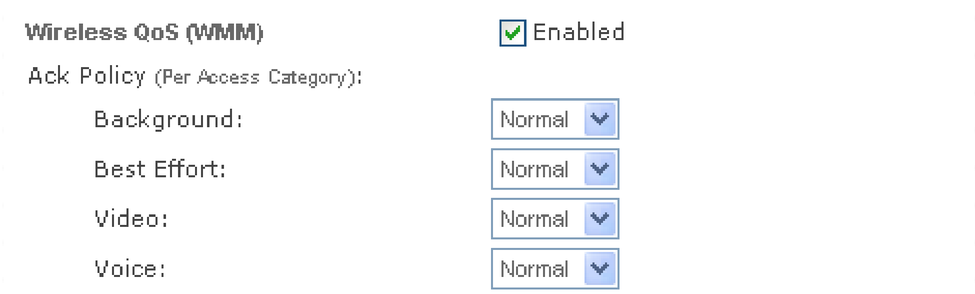


Figure 6.106 Wireless QoS (WMM)

> Note: When working in 802.11n mode, this feature's check box is not available as WMM is already enabled.

Background, Best Effort, Video and Voice are access categories for packet prioritization. Upon enabling WMM, the highest priority is given to Voice packets, decreasing towards Background packets which receive the lowest priority. In addition, you can control the reliability of traffic flow.

By default, the 'Ack Policy' for each access category is set to "Normal", meaning that an acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. You may choose to cancel the acknowledgement by selecting "No Ack" in the drop-down menu of each access category, thus changing the Ack policy. This can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.

6.4.6.6.7 Transmission Properties

Use this section to define the wireless transmission settings.

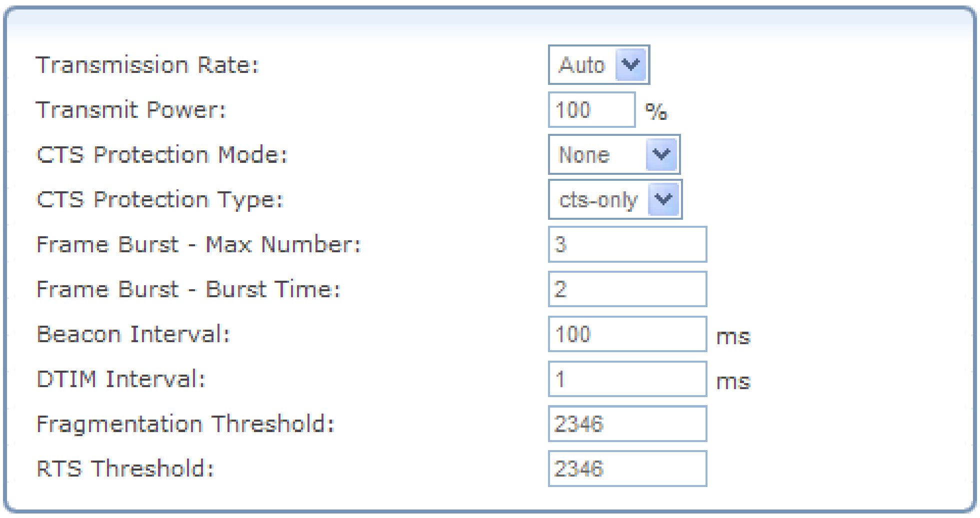


Figure 6.107 Transmission Properties

Transmission Rate The transmission rate is set according to the speed of your wireless connection. Select the transmission rate from the drop-down menu, or select 'Auto' to have OpenRG automatically use the fastest possible data transmission rate (the only option when

using 802.11ng). Note that if your wireless connection is weak or unstable, it is best to select a low transmission rate.

Transmit Power The percentage of maximum transmission power.

CTS Protection Mode CTS Protection Mode boosts your gateway's ability to intercept 802.11g and 802.11b transmissions. Conversely, CTS Protection Mode decreases performance. Leave this feature disabled unless you encounter severe communication difficulties between the gateway and 802.11g products. If enabling, select "Always". Select "Auto" to have OpenRG automatically decide whether or not to use this feature.

CTS Protection Type Select the type of CTS protection—cts-only or rts-cts.

Frame Burst This feature (also known as *packet bursting*) increases the speed of a 802.11g-based wireless network by unwrapping short packets and rebundling them into a larger one.

Note: This feature is only supported by the Atheros wireless cards.

- **Frame Burst – Max Number** At any given time, only one wireless client can communicate with the access point. Therefore, clients, competing for air time, transmit data in frame bursts. Use this field to determine the maximum number of frames that OpenRG will allow clients to transmit in a single frame burst.

- **Frame Burst – Burst Time** The maximum length of a frame burst. Limit the time of a frame burst to avoid large frames from taking communication precedence.

Beacon Interval A beacon is a packet broadcast by OpenRG to synchronize the wireless network. The Beacon Interval value indicates how often the beacon is sent.

DTIM Interval The Delivery Traffic Indication Message (DTIM) is a countdown value that informs wireless clients of the next opportunity to receive multicast and broadcast messages. This value ranges between 1 and 16384.

Fragmentation Threshold Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.

RTS Threshold OpenRG sends Request to Send (RTS) packets to the wireless client in order to negotiate the dispatching of data. The wireless client responds with a Clear to Send (CTS) packet, signaling that transmission can commence. In case packets are smaller than the preset threshold, the RTC/CTS mechanism is not active. If you encounter inconsistent data flow, try a minor reduction of the RTS threshold size.

6.4.6.6.8 Virtual Access Points

You can set up multiple virtual wireless LANs on OpenRG, limited only to the number supported by your wireless card. Such virtual wireless LANs are referred to as "Virtual APs" (virtual access points).

Note: Different wireless cards support a different number of virtual access points. The scenarios depicted herein refer to the **Ralink RT-2561** wireless card, supporting up to four virtual wireless access points.

The 'Virtual APs' section appears under the 'Wireless' sub-tab of the 'LAN Wireless 802.11g Access Point Properties' screen, and displays OpenRG's physical wireless access point, on top of which virtual connections may be created.

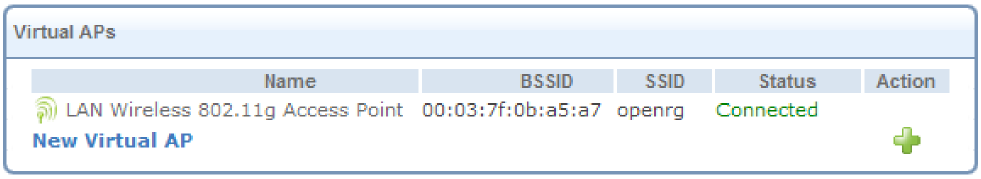


Figure 6.108 Virtual APs

To create a virtual connection, click the 'New Virtual AP' link. The screen refreshes, displaying the new virtual connection.

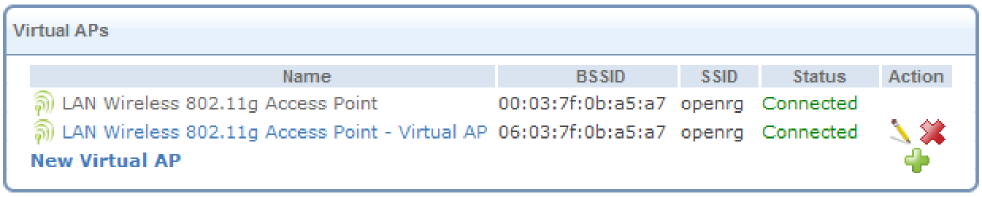


Figure 6.109 New Virtual Access Point

The new connection will also be added to the network connections list, and will be configurable like any other connection.

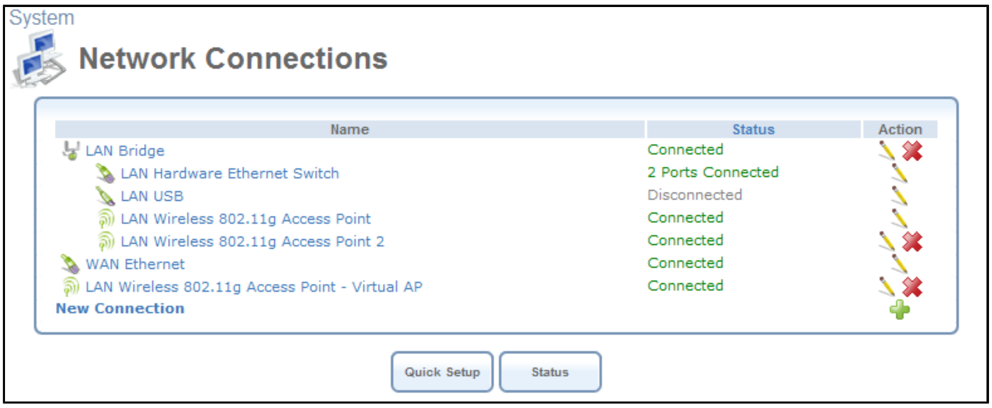


Figure 6.110 Network Connections

You can edit the new virtual access point's properties by clicking its action icon . The 'LAN Wireless 802.11g Access Point - Virtual AP Properties' screen appears. For example, change the connection's default name by changing the SSID value in the 'Wireless' sub-tab.

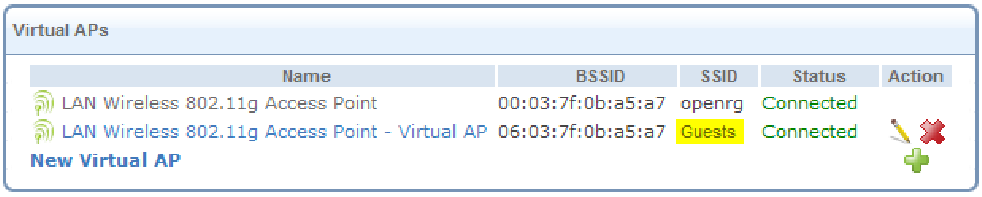


Figure 6.111 LAN Wireless 802.11g Access Point – Virtual AP Properties

A usage example for this virtual connection is to dedicate it for guest access. Through this connection, guests will be able to access the WAN, but they will be denied access to other wireless LANs provided by OpenRG. To do so, perform the following:

1. Set a firewall rule that blocks access to all other OpenRG LANs.

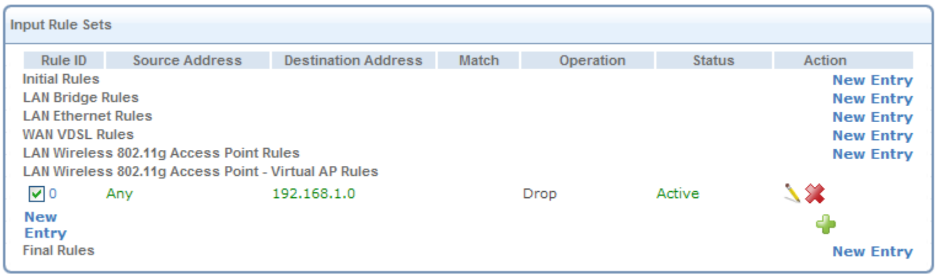


Figure 6.112 Firewall Rule

To learn how to do so, refer to Section 5.2.7.

2. Back in the virtual connection's 'LAN Wireless 802.11g Access Point - Virtual AP Properties' screen:

   a. In the 'Internet Protocol' section under the 'Settings' sub-tab, enter an IP address for the connection by selecting 'Use the Following IP Address'.

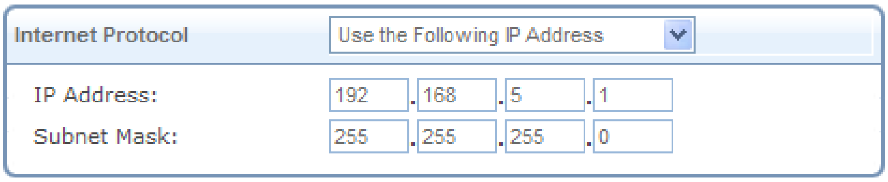


Figure 6.113 Internet Protocol

   b. In the 'IP Address Distribution' section, select 'DHCP Server' and enter the IP range from which IP addresses will be granted to wireless guests.

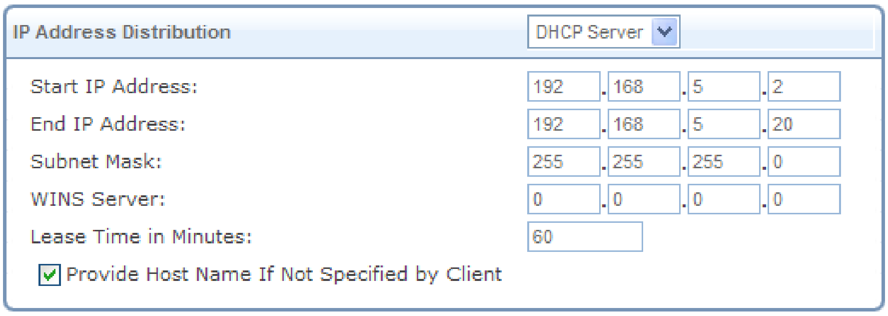


Figure 6.114 IP Address Distribution

c. Click 'OK' to save the settings.

After going through this procedure, you have secured all of your wireless connections. A guest will only be able to connect to the "Guests" wireless LAN, from which only the WAN access will be granted.

6.4.6.6.9 Advanced

Use the 'Advanced' sub-tab to configure the following parameters.

- **Internet Connection Firewall** Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

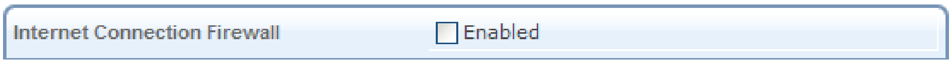


Figure 6.115 Internet Connection Firewall

- **Additional IP Addresses** You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://openrg.home.

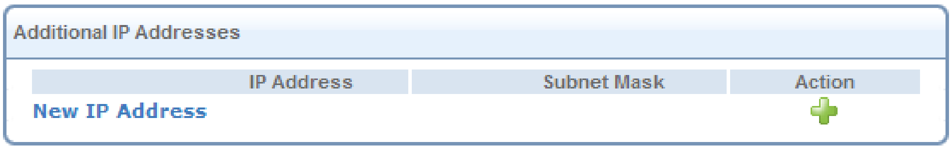


Figure 6.116 Additional IP Addresses

6.4.6.7 Supported Wireless Extension Cards

OpenRG currently supports the following wireless extension cards:

- Airgo AGN-100
- Ralink 802.11b/g

    - RT-2560
    - RT-2561
    - RT-2661
- Ralink 802.11n
    - RT-2860 (supported on Ikanos and Infineon platforms only)
- Atheros 802.11b/g (AR5212)
    - AR2413
    - AR2417
    - AR5413
- Atheros 802.11n (AR5416)

In addition, OpenRG supports Broadcom's built-in wireless chipset on the following platforms:

- Broadcom BCM96358
- ASUS 6020VI

Note that not all of the wireless features depicted in this section may be available with your version. OpenRG incorporates a wireless card auto-detection mechanism. When booting, OpenRG checks whether a wireless extension card is available. If so, it verifies the make and model of the card and only loads its supported wireless features. OpenRG will display a "Wireless" section in the 'Quick Setup' management screen. If your gateway includes a supported wireless module, yet you do not see this section, you will need to load a firmware version with wireless support.

6.4.7 Setting Up a WAN Ethernet Connection

The WAN Ethernet connection enables you to connect OpenRG to another network either directly or via an external modem. The Connection Wizard provides a number of methods for quick establishment of this connection.

6.4.7.1 Using the Ethernet Connection Wizard

The Ethernet Connection wizard utility is the most basic method for establishing a WAN Ethernet connection. This method is intended for connections that do not require username and password in order to connect to the Internet.

To establish a new Ethernet connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see Figure 6.15).

3. Select the 'External Cable Modem' radio button and click 'Next'. The 'Internet Cable Modem Connection' screen appears.

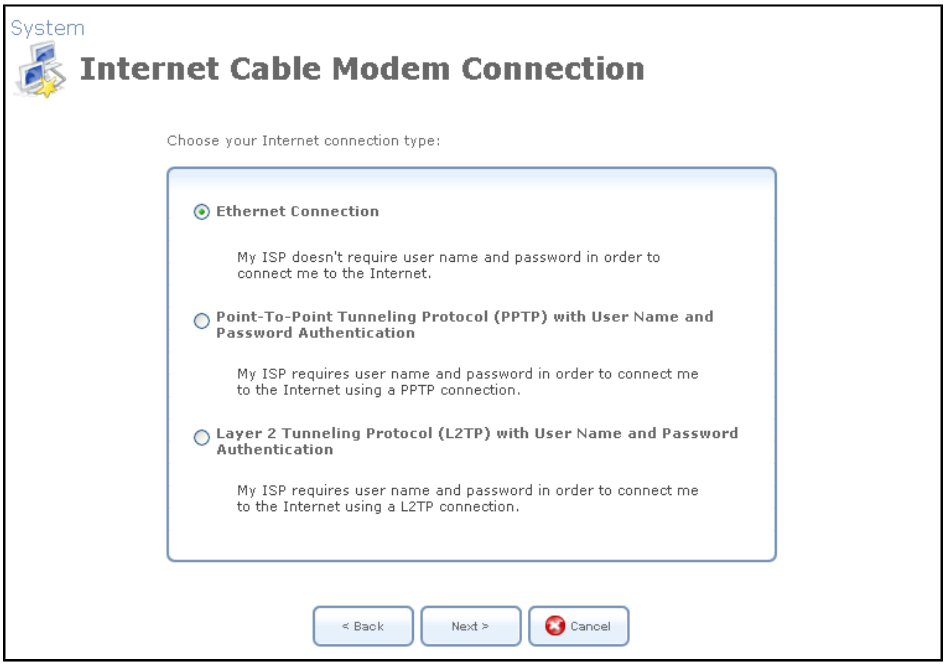


Figure 6.117 Internet Cable Modem Connection

4. Select the 'Ethernet Connection' radio button and click 'Next'. The 'Connection Summary' screen appears.

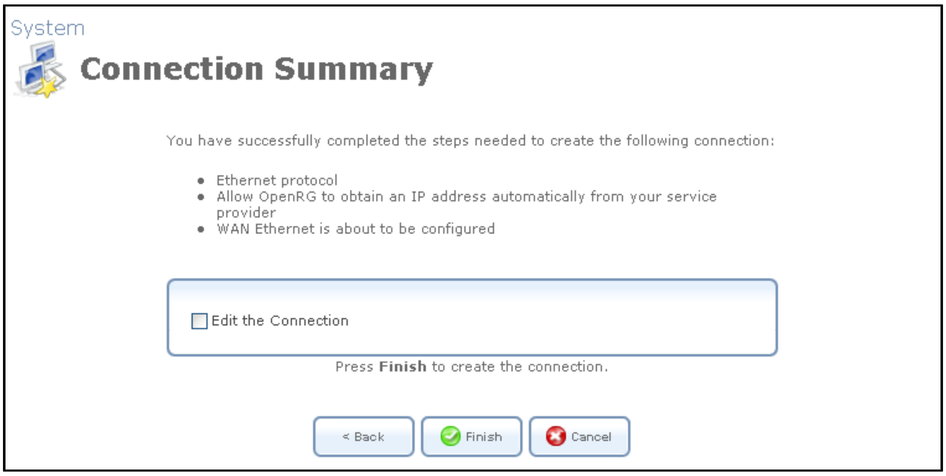


Figure 6.118 Connection Summary

5. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

6. Click 'Finish' to save the settings.

The WAN Ethernet connection will be configured accordingly. Refer to Section 6.4.7.4 to learn how to view and edit the connection's settings.

6.4.7.2 Using the Dynamic Host Configuration Protocol (DHCP) Wizard

The Dynamic Host Configuration Protocol (DHCP) connection wizard utility is a dynamic negotiation method for establishing a WAN Ethernet connection. When using this method, the client obtains an IP address automatically from the service provider when connecting to the Internet.

To create a new WAN DHCP-based connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears (see Figure 6.14).
2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see Figure 6.15).
3. Select the 'Ethernet Connection' radio button and click 'Next'. The 'Ethernet Connection' screen appears.

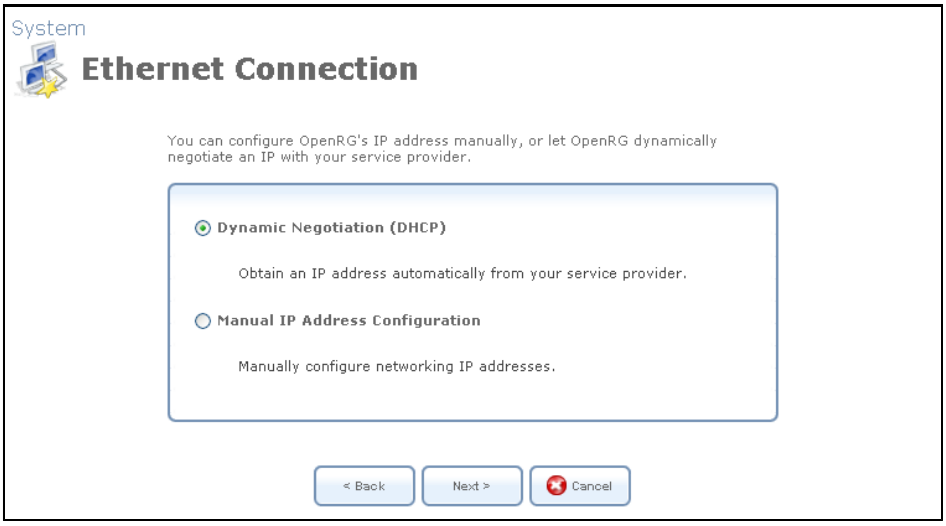


Figure 6.119 Ethernet Connection

4. Select the 'Dynamic Negotiation (DHCP)' radio button and click 'Next'. The 'Connection Summary' screen appears.

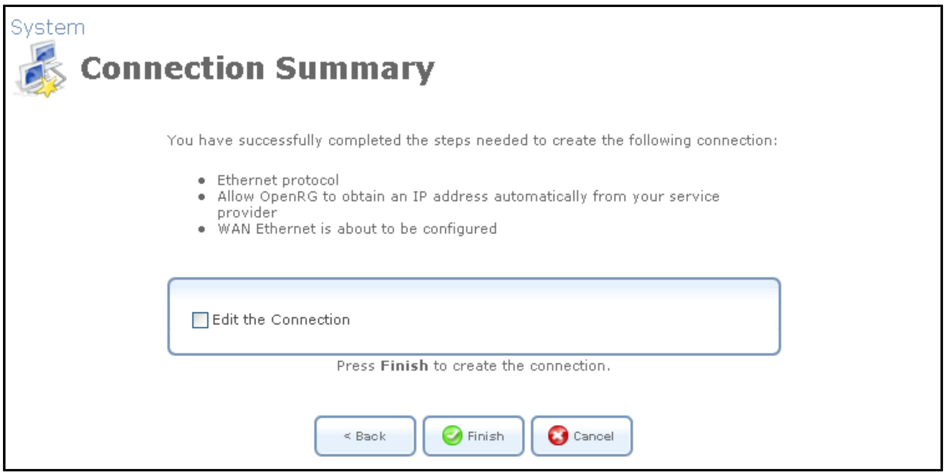


Figure 6.120 Connection Summary

5. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

6. Click 'Finish' to save the settings.

The WAN Ethernet connection will be configured to obtain an IP address using a DHCP. Refer to Section 6.4.7.4 to learn how to view and edit the connection's settings.

Note: If your WAN connection is set to DHCP when there is no DHCP server available, and a PPPoE server is available instead, the device status will show: "Waiting for DHCP Lease – PPPoE server found, consider configuring your WAN connection to PPPoE". If you select this option, refer to Section 6.4.8.

6.4.7.3 Using the Manual IP Address Configuration Wizard

The Manual IP Address Configuration wizard utility is used to manually configure the WAN interface's IP addresses when connecting to the Internet.

To manually configure the IP addresses, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see Figure 6.15).

3. Select the 'Ethernet Connection' radio button and click 'Next'. The 'Ethernet Connection' screen appears.

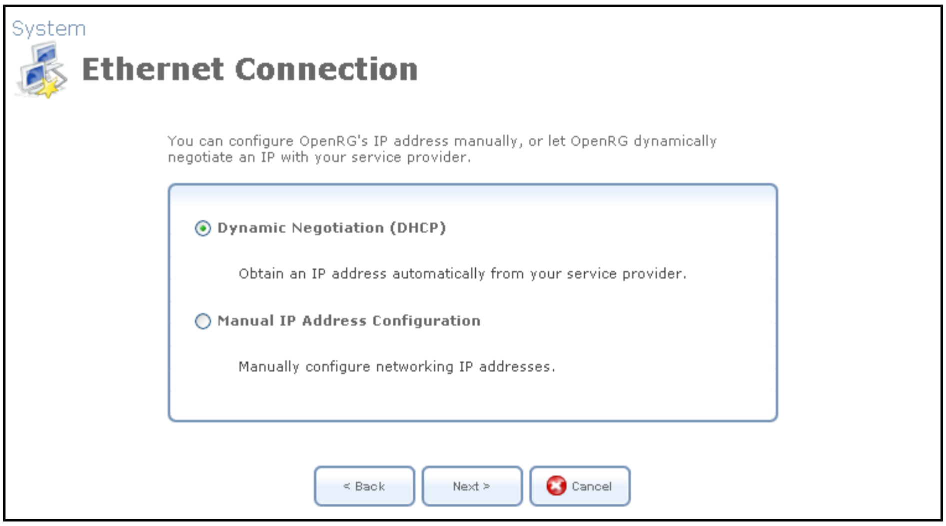


Figure 6.121 Ethernet Connection

4. Select the 'Manual IP Address Configuration' radio button and click 'Next'. The 'Manual IP Address Configuration' screen appears.

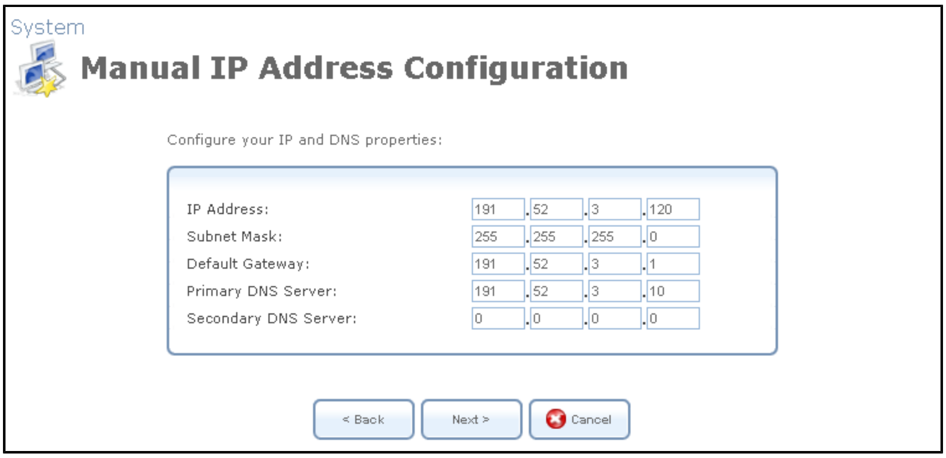


Figure 6.122 Manual IP Address Configuration

5. Enter the IP address, subnet mask, default gateway, and DNS server addresses in their respective fields. These values should either be provided to you by your ISP or configured by your system administrator.

6. Click 'Next'. The 'Connection Summary' screen appears.

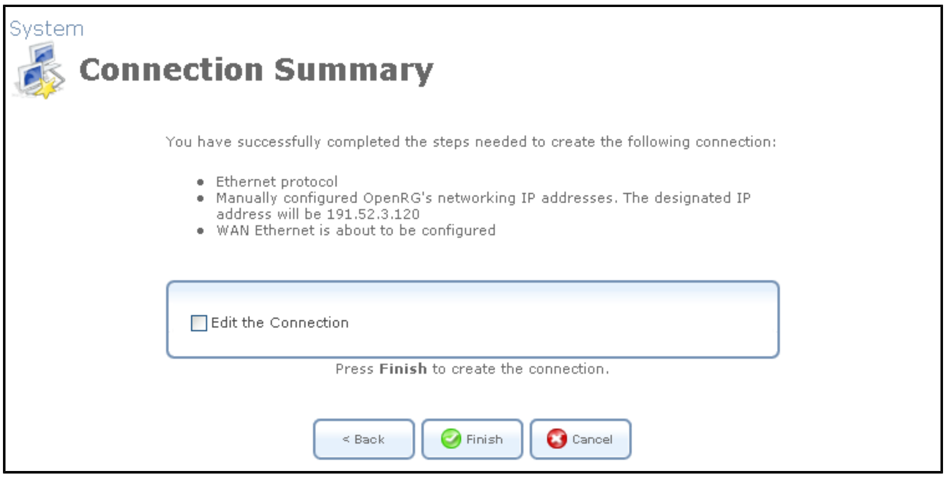


Figure 6.123 Connection Summary

7. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

8. Click 'Finish' to save the settings.

The WAN Ethernet connection will be configured with the new settings. Refer to Section 6.4.7.4 to learn how to view and edit the connection's settings.

6.4.7.4 Viewing and Editing the Connection's Settings

To view and edit the WAN Ethernet connection settings, click the 'WAN Ethernet' link in the 'Network Connections' screen (see Figure 6.13). The 'WAN Ethernet Properties' screen appears.

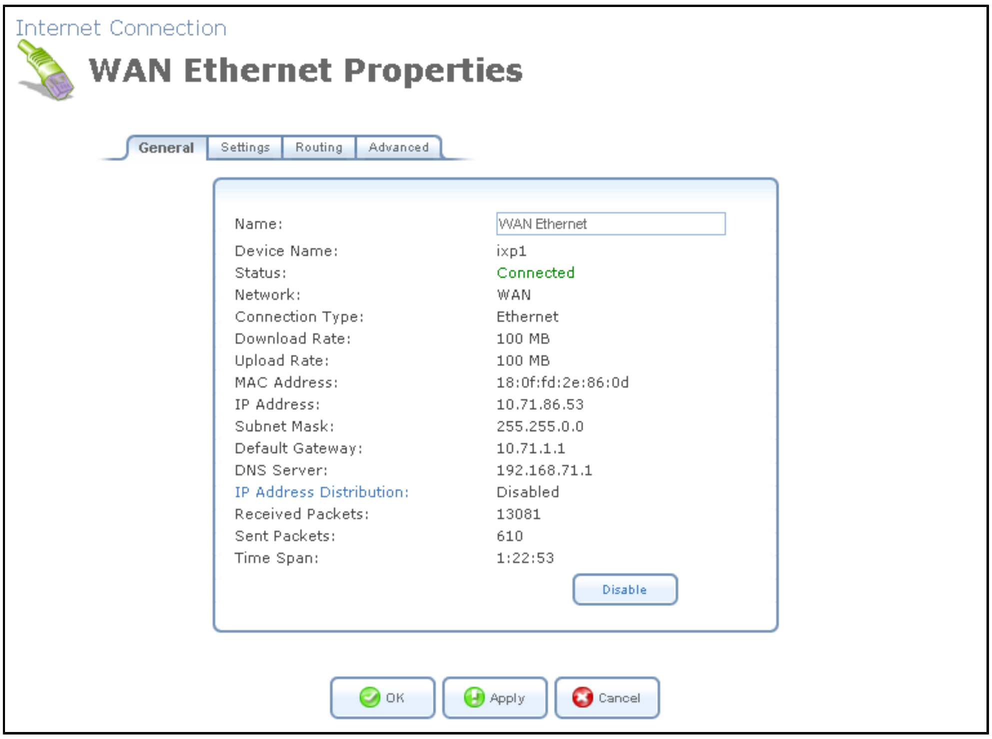


Figure 6.124 WAN Ethernet Properties

6.4.7.4.1 General

This sub-tab enables you to view the WAN Ethernet connection settings (see Figure 6.124). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.7.4.2 Settings

This sub-tab enables you to configure the following WAN Ethernet settings:

General It is recommended not to change the default values unless you are familiar with the networking concepts they represent. Since your gateway is configured to operate with the default values, no parameter modification is necessary.

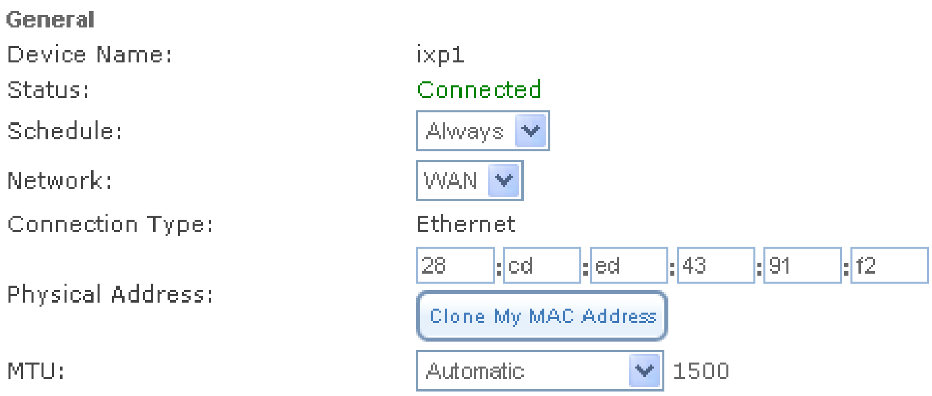


Figure 6.125 General

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

Clone My MAC Address Press this button to copy your PC's current MAC address to the board.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen will refresh to display relevant configuration settings according to your choice.

No IP Address Select 'No IP Address' if you require that your gateway have no IP address. This can be useful if you are working in an environment where you are not connected to other networks, such as the Internet.

Figure 6.126 Internet Protocol – No IP Address

Obtain an IP Address Automatically Your connection is configured by default to act as a DHCP client. You should keep this configuration in case your service provider supports

DHCP, or if you are connecting using a dynamic IP address. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead. You can click the 'Release' button to release the current leased IP address. Once the address has been released, the button text changes to 'Renew'. Use the 'Renew' button to renew the leased IP address.

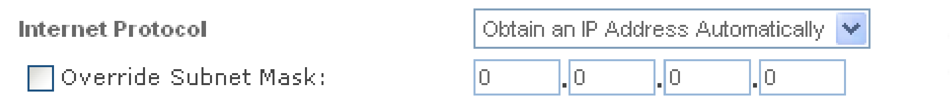


Figure 6.127 Internet Protocol Settings – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

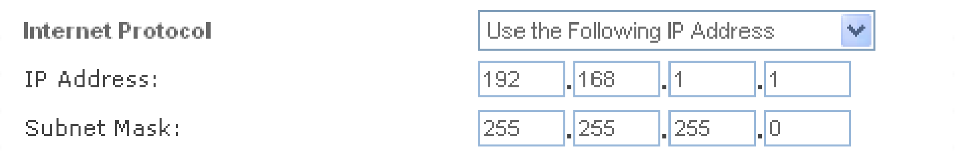


Figure 6.128 Internet Protocol – Static IP

DNS Server Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 6.129 DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

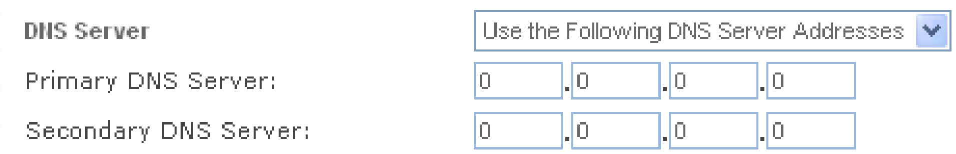


Figure 6.130 DNS Server – Static IP

To learn more about this feature, refer to Section 5.12.1.

IP Address Distribution The 'IP Address Distribution' section allows you to configure the gateway's Dynamic Host Configuration Protocol (DHCP) server parameters. The DHCP automatically assigns IP addresses to network PCs. If you enable this feature, make sure that

you also configure your network PCs as DHCP clients. For a comprehensive description of this feature, refer to Section 5.11. Select one of the following options from the 'IP Address Distribution' drop-down menu:

- **DHCP Server**

  In case you have chosen DHCP Server, complete the following fields:

  Start IP Address The first IP address that may be assigned to a LAN host. Since the LAN interface's default IP address is 192.168.1.1, it is recommended that the first address assigned to a LAN host will be 192.168.1.2 or greater.

  End IP Address The last IP address in the range that can be used to automatically assign IP addresses to LAN hosts.

  Subnet Mask A mask used to determine to what subnet an IP address belongs. An example of a subnet mask value is 255.255.255.0.

  Lease Time In Minutes Each device will be assigned an IP address by the DHCP server for this amount of time, when it connects to the network. When the lease expires the server will determine if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use will become available for other computers on the network.

  Provide Host Name If Not Specified by Client If the DHCP client does not have a host name, the gateway will automatically assign one for it.

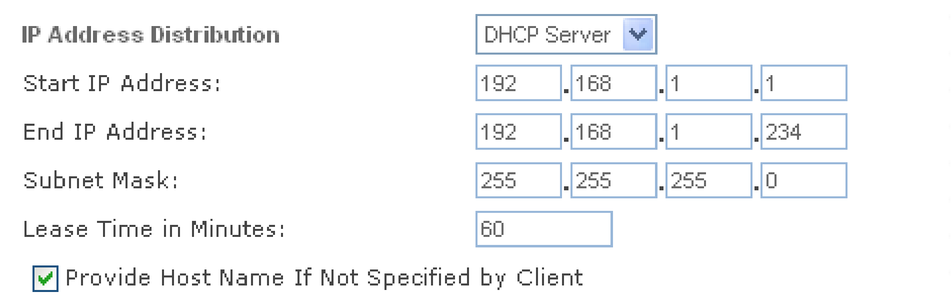


Figure 6.131 IP Address Distribution – DHCP Server

- **Disabled** Select 'Disabled' from the drop-down menu if you would like to statically assign IP addresses to your network computers.

Figure 6.132 IP Address Distribution – Disable DHCP

6.4.7.4.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts

how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

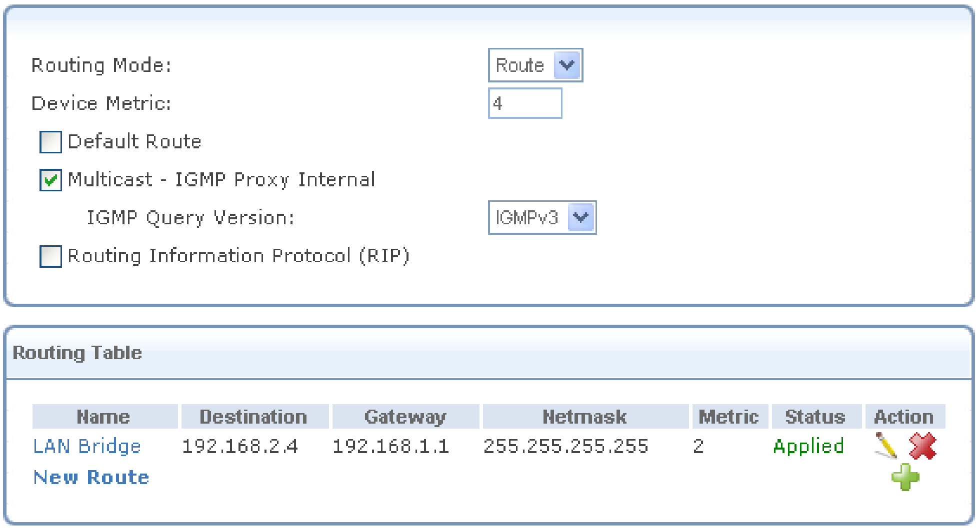


Figure 6.133 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
- **Send RIP messages**—select either 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.

Routing Table Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.
To learn more about this feature, refer to Section 6.6.

6.4.7.4.4 IPv6

This subtab enables you to define new IPv6 addresses for the current connection, by clicking the 'New Unicast Address' link. Note that this sub-tab appears only if the IPv6 feature is enabled on the gateway. For more information, refer to Section 6.6.2.

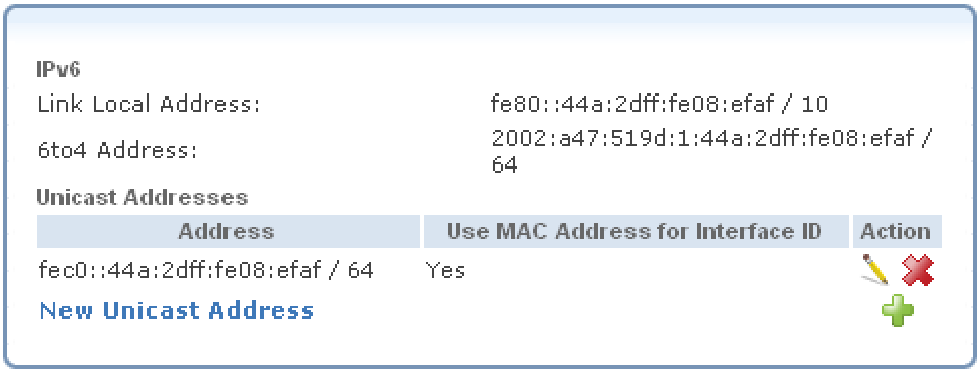


Figure 6.134 IPv6 Settings

6.4.7.4.5 Advanced

This sub-tab enables you to configure the advanced WAN Ethernet settings.

- **Internet Connection Firewall** Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

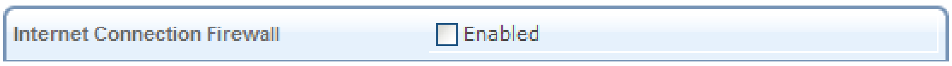


Figure 6.135 Internet Connection Firewall

Internet Connection Fastpath Select this check box to utilize the *Fastpath* algorithm for enhancing packet flow, resulting in faster communication between the LAN and the WAN. By default, this feature is enabled.

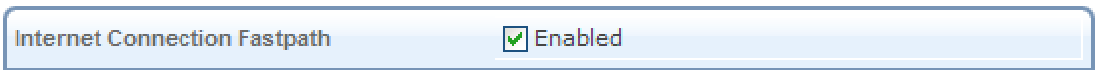


Figure 6.136 Internet Connection Fastpath

- **Additional IP Addresses** You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://openrg.home.

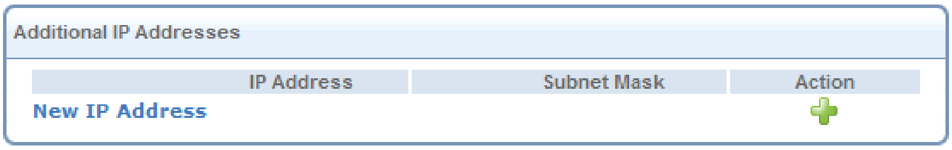


Figure 6.137 Additional IP Addresses

6.4.8 Setting Up a PPPoE Connection

Point-to-Point Protocol over Ethernet (PPPoE) relies on two widely accepted standards, PPP and Ethernet. PPPoE enables your home network PCs that communicate on an Ethernet network to exchange information with PCs on the Internet. PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the multipoint architecture of Ethernet. A discovery process in PPPoE determines the Ethernet MAC address of the remote device in order to establish a session.

6.4.8.1 Creating a PPPoE Connection

To create a PPPoE connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see Figure 6.15).

3. Select the 'External DSL Modem' radio button and click 'Next'. The 'Point-to-Point Protocol over Ethernet' screen appears.

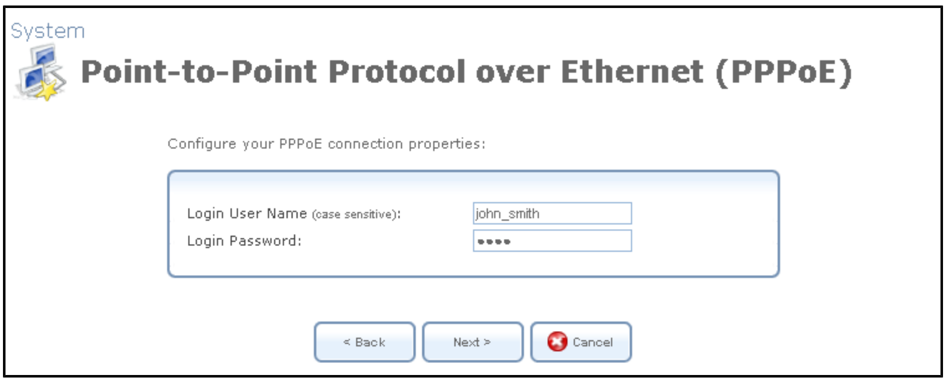


Figure 6.138 Point-to-Point Protocol over Ethernet

4. Enter the username and password provided by your Internet Service Provider (ISP), and click 'Next'. The 'Connection Summary' screen appears.

Figure 6.139 Connection Summary

5. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

6. Click 'Finish' to save the settings.

The new PPPoE connection will be added to the network connections list, and will be configurable like any other connection.

Note: If your WAN connection is set to PPPoE when there is no PPPoE server available, and a DHCP server is available instead, the device status will show: "In Progress – DHCP server found, consider configuring your WAN connection to Automatic".

6.4.8.2 Viewing and Editing the Connection's Settings

To view and edit the PPPoE connection settings, click the 'WAN PPPoE' link in the 'Network Connections' screen (see Figure 6.13). The 'WAN PPPoE Properties' screen appears.

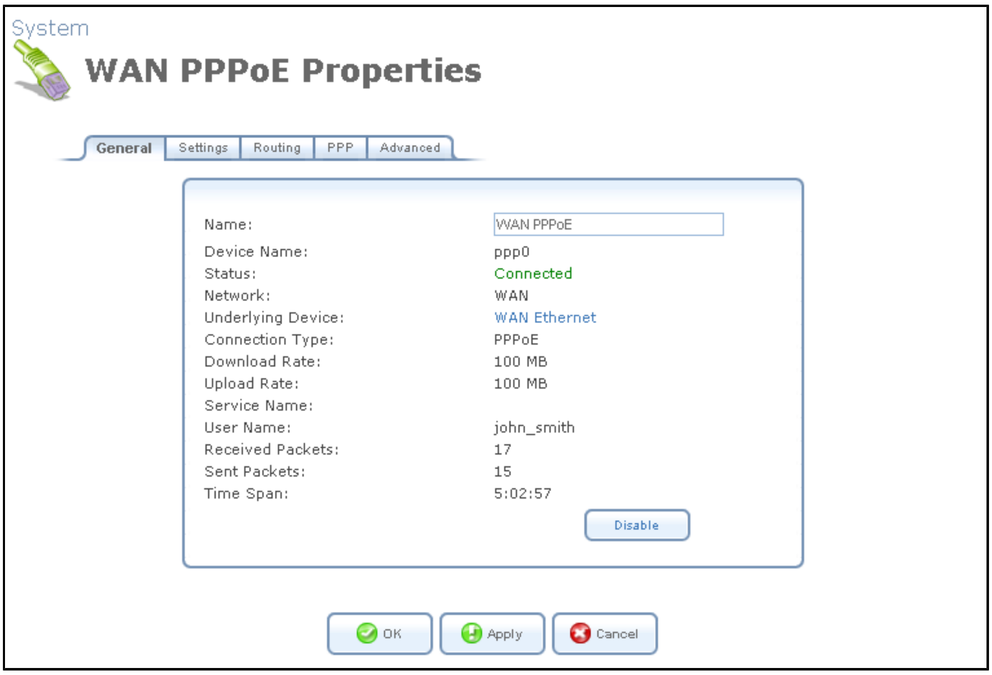


Figure 6.140 WAN PPPoE Properties

6.4.8.2.1 General

This sub-tab enables you to view the PPPoE connection settings (see Figure 6.140). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.8.2.2 Settings

This sub-tab enables you to edit the following PPPoE connection settings:

General This section displays the connection's general parameters.

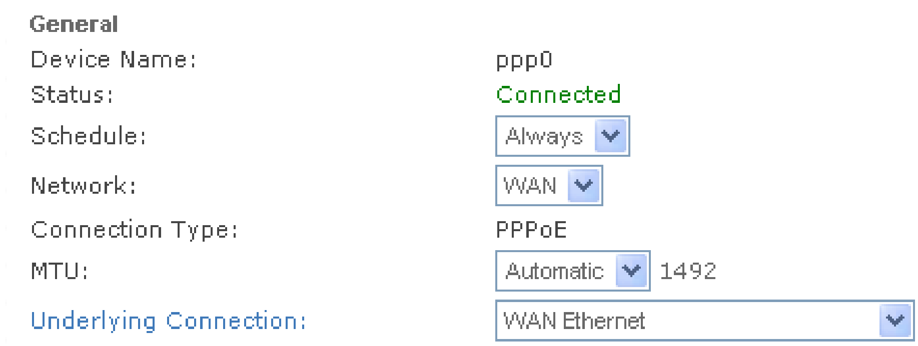


Figure 6.141 General PPPoE Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more

information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Underlying Connection Specify the underlying connection above which the protocol will be initiated.

ATM

Asynchronous Transfer Mode (ATM) is a network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with other technologies. The small, constant cell size allows the transmission of video, audio, and computer data, assuring that no single type of data consumes the connection. ATM addressing consists of two identifiers that identify the virtual path (VPI) and the virtual connection (VCI). A virtual path consists of multiple virtual channels to the same endpoint. The 'Encapsulation' for connection should be set to either 'LLC' or 'VCMux'. You should configure these parameters according to the information provided by your ISP.

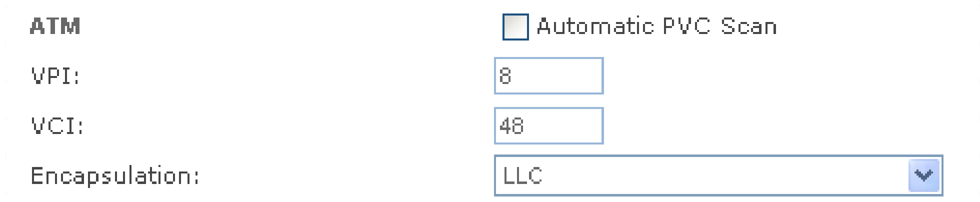


Figure 6.142 ATM Settings

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' combo-box:

- Unnumbered
- Obtain an IP Address Automatically
- Use the Following IP Address

Please note that the screen will refresh to display relevant configuration settings according to your choice.

Unnumbered Select this option to assign a predefined LAN address as OpenRG's WAN address. This is useful when OpenRG operates in routing mode. Before selecting this option, configure the 'Internet Protocol' of your LAN device (or bridge, in case the LAN device is under a bridge) to use a permanent (static) IP address from the range of IP addresses provided by your ISP (instead of 192.168.1.1).

Figure 6.143 Internet Protocol – Unnumbered

Obtain an IP Address Automatically Your connection is configured by default to obtain an IP automatically. You should change this configuration in case your service provider requires it. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead.

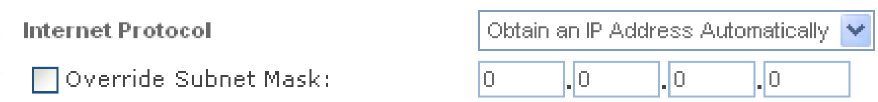


Figure 6.144 Internet Protocol – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

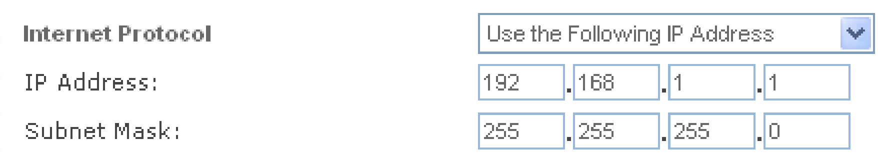


Figure 6.145 Internet Protocol – Static IP

DNS Server Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 6.146 DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

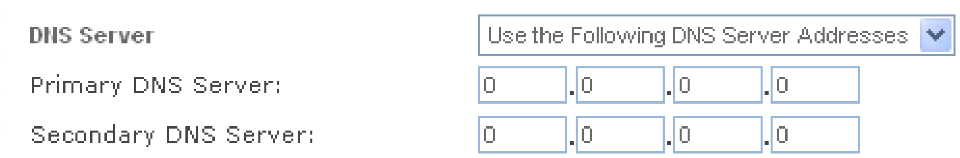


Figure 6.147 DNS Server – Static IP

To learn more about this feature, refer to Section 5.12.1.

6.4.8.2.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

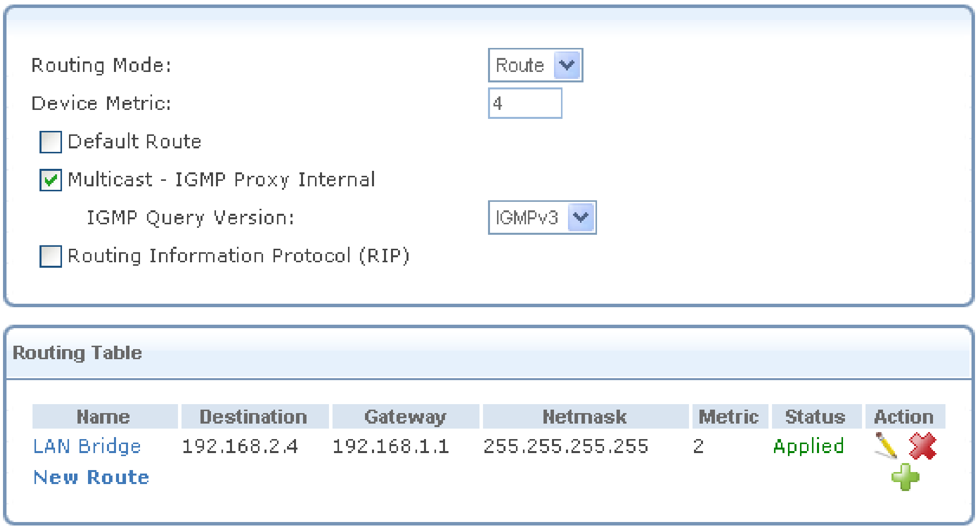


Figure 6.148 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
- **Send RIP messages**—select either 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.

Routing Table Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.
To learn more about this feature, refer to Section 6.6.

6.4.8.2.4 PPP

Point-to-Point Protocol (PPP) is the most popular method for transporting packets between the user and the Internet service provider. PPP supports authentication protocols such as PAP and CHAP, as well as other compression and encryption protocols.

Service Name Specify the networking peer's service name, if provided by your ISP.

PPP-on-Demand Use PPP on demand to initiate the point-to-point protocol session only when packets are actually sent over the Internet.

Time Between Reconnect Attempts Specify the duration between PPP reconnected attempts, as provided by your ISP.

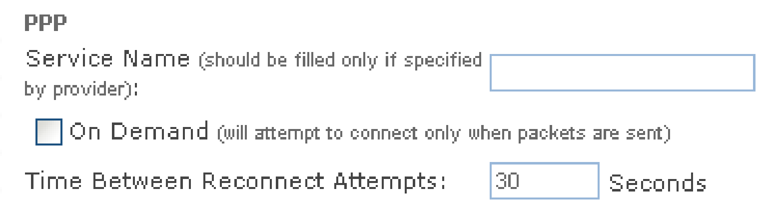


Figure 6.149 PPP Configuration

PPP Authentication Point-to-Point Protocol (PPP) currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2. This section allows you to select the authentication protocols your gateway may use when negotiating with a PPTP server. Select all the protocols if no information is available about the server's authentication protocols. Note that encryption is performed only if 'Microsoft CHAP', 'Microsoft CHAP version 2', or both are selected.

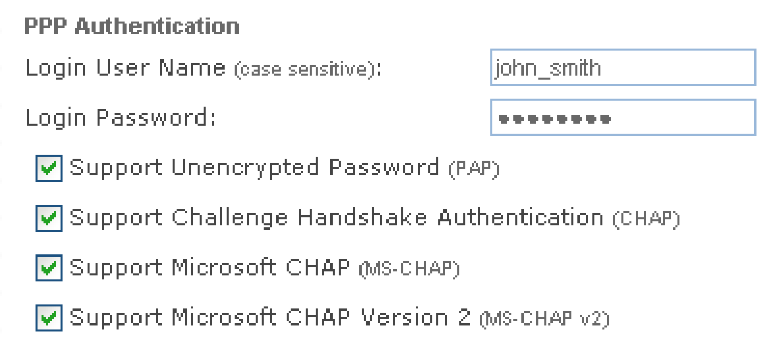


Figure 6.150 PPP Authentication

Login User Name As agreed with ISP.

Login Password As agreed with ISP.

Support Unencrypted Password (PAP) Password Authentication Protocol (PAP) is a simple, plain-text authentication scheme. The user name and password are requested by your networking peer in plain-text. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.

Support Challenge Handshake Authentication (CHAP) The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.

Support Microsoft CHAP Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.

Support Microsoft CHAP Version 2 Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.

PPP Compression The PPP Compression Control Protocol (CCP) is responsible for configuring, enabling, and disabling data compression algorithms on both ends of the point-to-point link. It is also used to signal a failure of the compression/ decompression mechanism in a reliable manner.

Figure 6.151 PPP Compression

For each compression algorithm, select one of the following from the drop down menu:

Reject Reject PPP connections with peers that use the compression algorithm.

Allow Allow PPP connections with peers that use the compression algorithm.

Require Ensure a connection with a peer is using the compression algorithm.

6.4.8.2.5 Advanced

This sub-tab enables you to edit the advanced PPPoE connection settings.

- **Internet Connection Firewall** Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

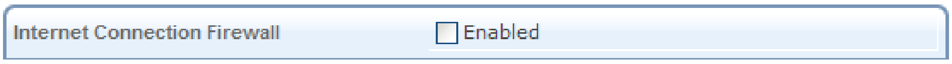


Figure 6.152 Internet Connection Firewall

Internet Connection Fastpath Select this check box to utilize the *Fastpath* algorithm for enhancing packet flow, resulting in faster communication between the LAN and the WAN. By default, this feature is enabled.

Figure 6.153 Internet Connection Fastpath

6.4.9 Setting Up an L2TP Connection

Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol, enabling your gateway to create VPN connections. Derived from Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) technology, L2TP encapsulates PPP frames into IP packets either at the remote user's PC or at an ISP that has an L2TP Remote Access Concentrator (LAC). The LAC transmits the L2TP packets over the network to the L2TP Network Server (LNS) at the corporate side. With OpenRG, L2TP is targeted at serving two purposes:

1. Connecting OpenRG to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established by authenticating your username and password.

2. Connecting OpenRG to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates, and user name and password for authentication.

6.4.9.1 Creating an L2TP Connection

To create a new L2TP connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see Figure 6.15).

3. Select the 'External Cable Modem' radio button (this option is for both internal and external cable modems) and click 'Next'. The 'Internet Cable Modem Connection' screen appears.

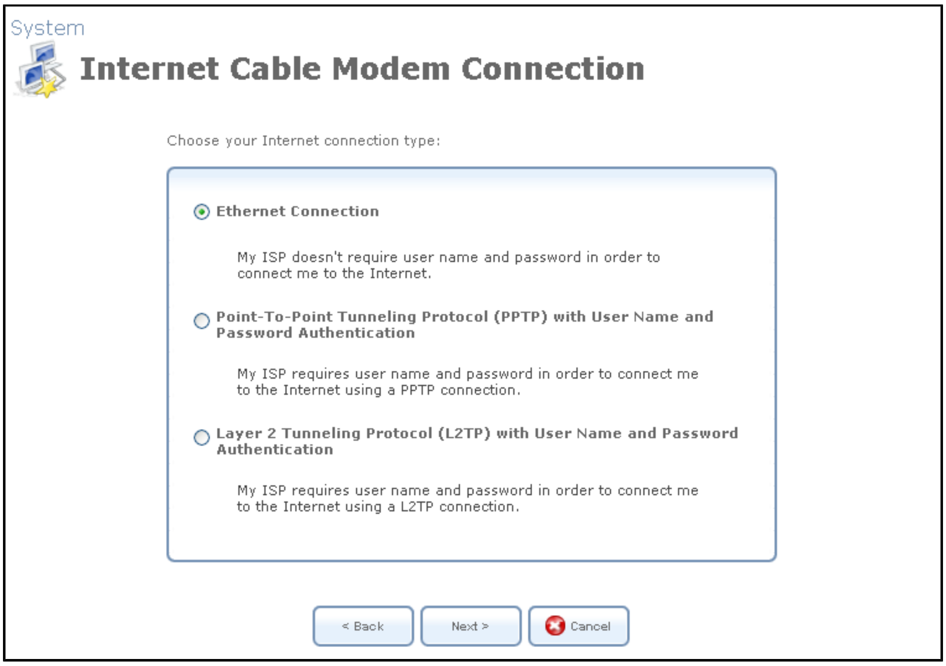


Figure 6.154 Internet Cable Modem Connection

4. Select the 'Layer 2 Tunneling Protocol (L2TP) with the 'User Name and Password Authentication' radio button and click 'Next'. The 'Layer 2 Tunneling Protocol (L2TP)' screen appears.

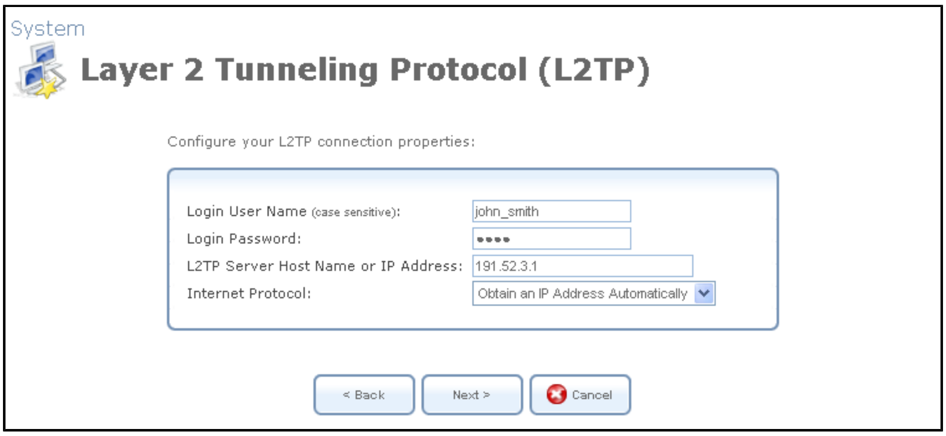


Figure 6.155 Layer 2 Tunneling Protocol (L2TP)

5. Enter the username and password provided by your Internet Service Provider (ISP).

6. Enter the L2TP server host name or IP address provided by your ISP.

7. Select whether to obtain an IP address automatically or specify one. This option is described in detail in Internet Protocol.

8. Click 'Next'. The 'Connection Summary' screen appears.

Figure 6.156 Connection Summary

9. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

10. Click 'Finish' to save the settings.

The new L2TP connection will be added to the network connections list, and will be configurable like any other connection.

6.4.9.2 Creating an L2TP IPSec VPN Connection

To create an L2TP IPSec VPN connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').

3. Select the 'VPN Client or Point-To-Point' radio button and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

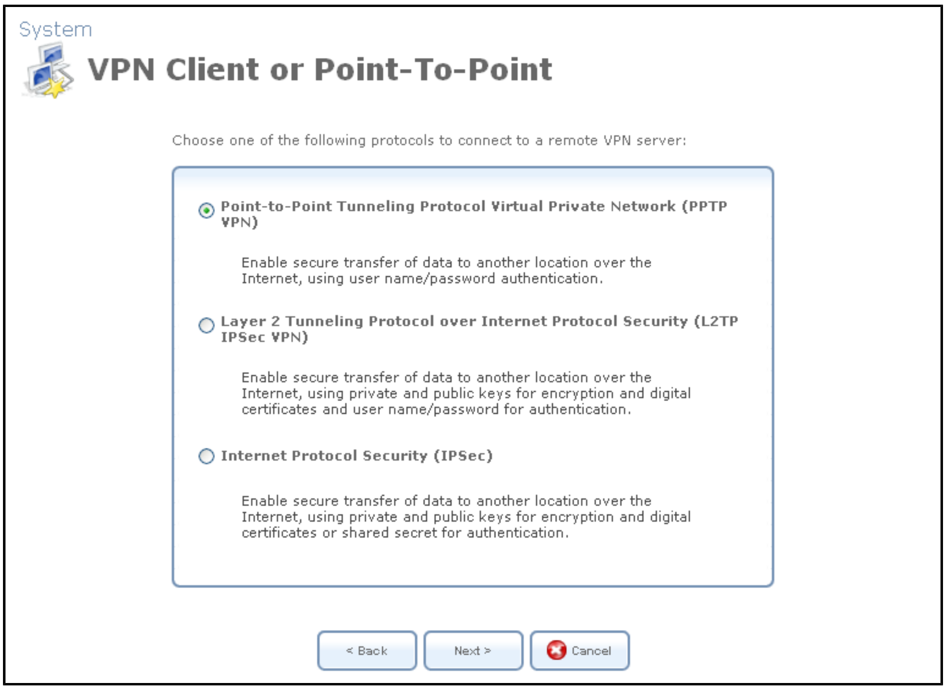


Figure 6.157 VPN Client or Point-To-Point

4. Select the 'Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)' radio button and click 'Next'. The 'Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)' screen appears.

Figure 6.158 Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)

5. Enter the username and password provided by the administrator of the network you are trying to access.

6. Enter the IPSec shared secret, which is the encryption key jointly decided upon with the network you are trying to access.

7. Enter the remote tunnel endpoint address. This would be the IP address or domain name of the remote network computer, which serves as the tunnel's endpoint.

8. Click 'Next'. The 'Connection Summary' screen appears.

Figure 6.159 Connection Summary

9. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

10. Click 'Finish' to save the settings.

The new L2TP IPSec VPN connection will be added to the network connections list, and will be configurable like any other connection.

6.4.9.3 Viewing and Editing the Connection's Settings

To view and edit the L2TP connection settings, click the 'L2TP' link in the 'Network Connections' screen (see Figure 6.13). The 'L2TP Properties' screen appears.

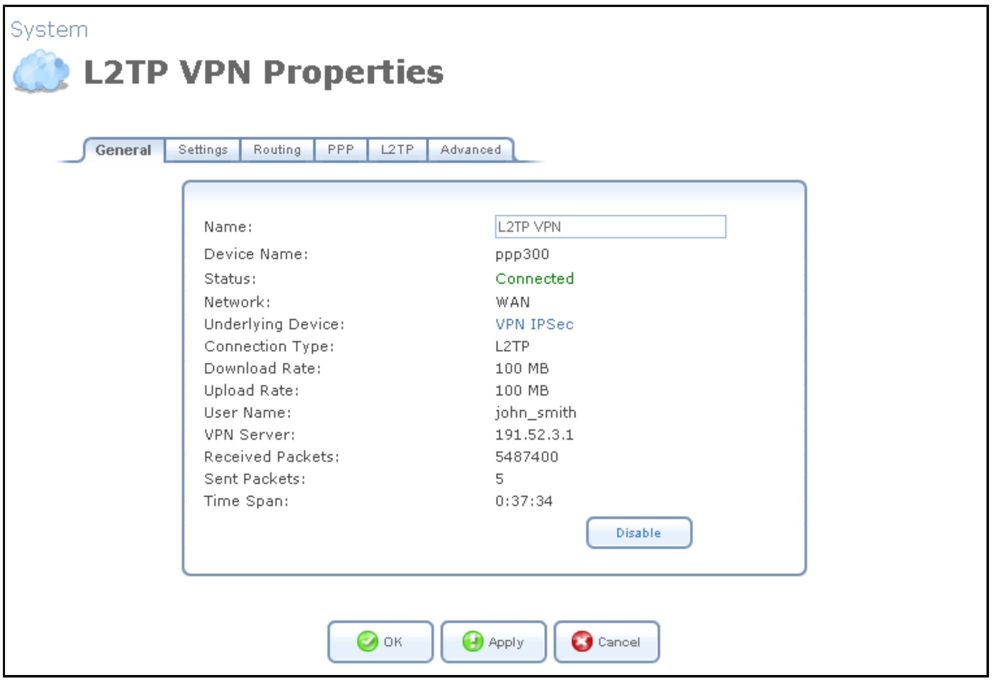


Figure 6.160 L2TP Properties

6.4.9.3.1 General

This sub-tab enables you to view a detailed summary of the connection's settings. These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.9.3.2 Settings

This sub-tab enables you to edit the following L2TP connection settings:

General This section displays the connection's general parameters.

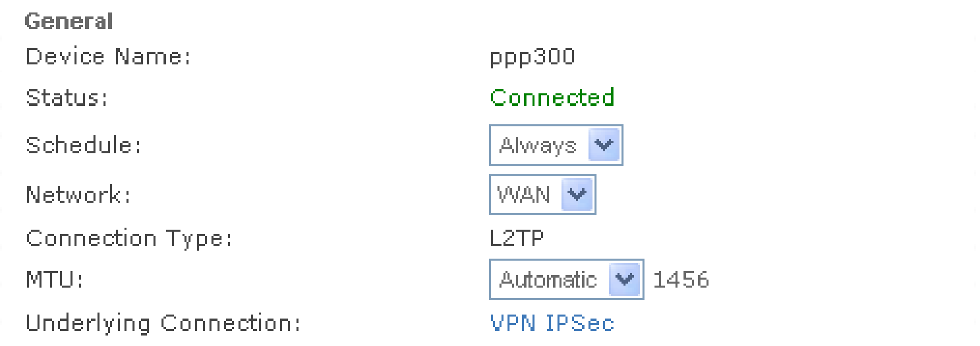


Figure 6.161 General L2TP Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- Obtain an IP Address Automatically

- Use the Following IP Address

Note that the screen refreshes to display relevant configuration settings according to your choice.

Obtain an IP Address Automatically Your connection is configured by default to obtain an IP automatically. You should change this configuration in case your service provider requires it. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead.

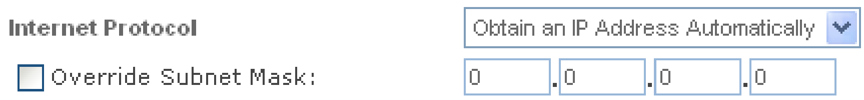


Figure 6.162 Internet Protocol – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

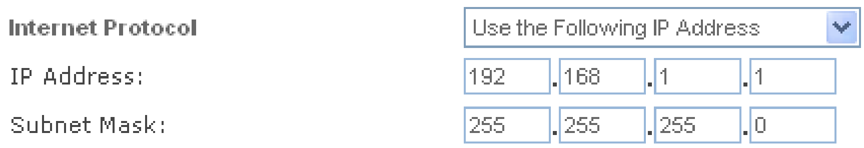


Figure 6.163 Internet Protocol – Static IP

DNS Server Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 6.164 DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

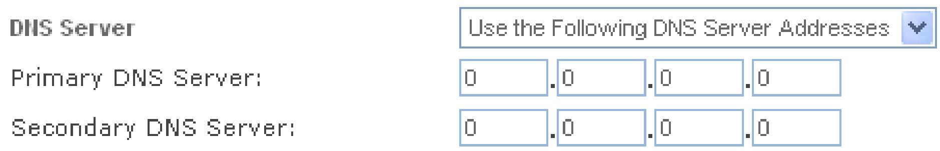


Figure 6.165 DNS Server – Static IP

To learn more about this feature, refer to Section 5.12.1.

6.4.9.3.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

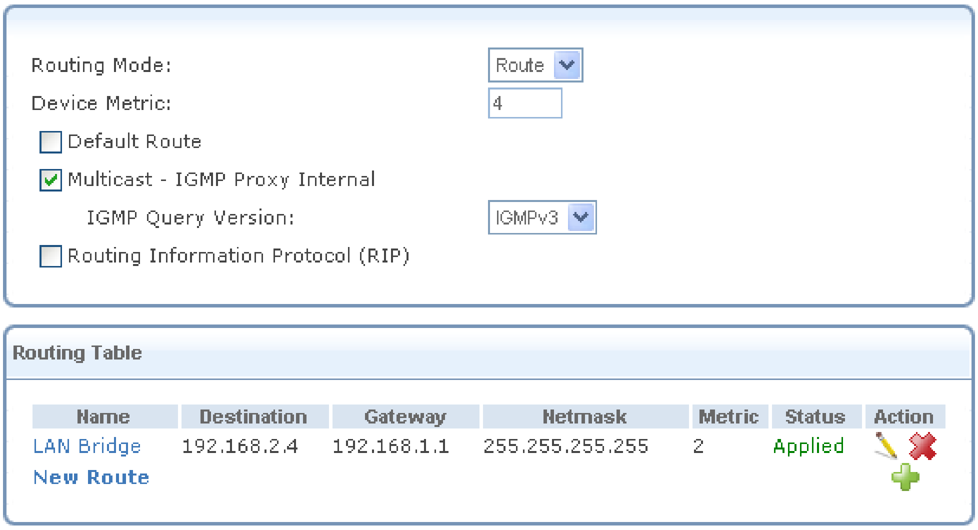


Figure 6.166 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

> **Route** Use route mode if you want your gateway to function as a router between two networks.
>
> **NAPT** Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

> **IGMP Query Version** OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
- **Send RIP messages**—select either 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.

Routing Table Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.
To learn more about this feature, refer to Section 6.6.

6.4.9.3.4 PPP

This sub-tab enables you to edit the following PPP settings.

PPP Point-to-Point Protocol (PPP) is the most popular method for transporting packets between the user and the Internet service provider. PPP supports authentication protocols such as PAP and CHAP, as well as other compression and encryption protocols.

PPP-on-Demand Use PPP on demand to initiate the point-to-point protocol session only when packets are actually sent over the Internet.

Time Between Reconnect Attempts Specify the duration between PPP reconnected attempts, as provided by your ISP.

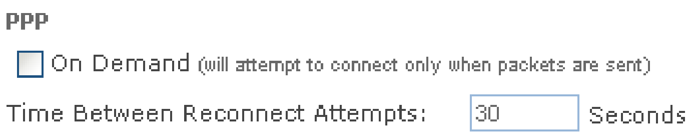


Figure 6.167 PPP Configuration

PPP Authentication Point-to-Point Protocol (PPP) currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2. This section allows you to select the authentication protocols your gateway may use when negotiating with a PPTP server. Select all the protocols if no information is available about the server's authentication protocols. Note that encryption is performed only if 'Microsoft CHAP', 'Microsoft CHAP version 2', or both are selected.

Figure 6.168 PPP Authentication

Login User Name As agreed with ISP.

Login Password As agreed with ISP.

Support Unencrypted Password (PAP) Password Authentication Protocol (PAP) is a simple, plain-text authentication scheme. The user name and password are requested by your networking peer in plain-text. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.

Support Challenge Handshake Authentication (CHAP) The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.

Support Microsoft CHAP Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.

Support Microsoft CHAP Version 2 Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.

PPP Encryption PPP supports encryption facilities to secure the data across the network connection. A wide variety of encryption methods may be negotiated, although typically only one method is used in each direction of the link. This section allows you to select the encryption methods your gateway may use when negotiating with a PPTP server. Select all the methods if no information is available about the server's encryption methods. Please note that PPP encryption can only be used with MS-CHAP or MS-CHAP-V2 authentication protocols.

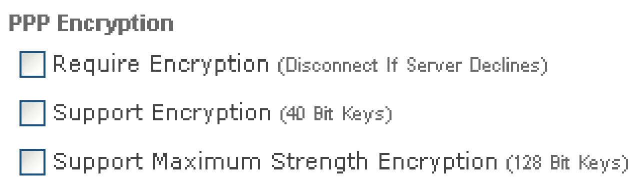


Figure 6.169 PPP Encryption

Require Encryption Select this check box to ensure that the PPP connection is encrypted.

Support Encryption (40 Bit Keys) Select this check box if your peer supports 40 bit encryption keys.

Support Maximum Strength Encryption (128 Bit Keys) Select this check box if your peer supports 128 bit encryption keys.

6.4.9.3.5 L2TP

This sub-tab enables you to edit the following L2TP settings.

L2TP Define your ISP's server parameters.

- **L2TP Server Host Name or IP Address** Enter the connection's host name or IP address obtained from your ISP.
- **Shared Secret** Enter the shared secret value obtained from your ISP.

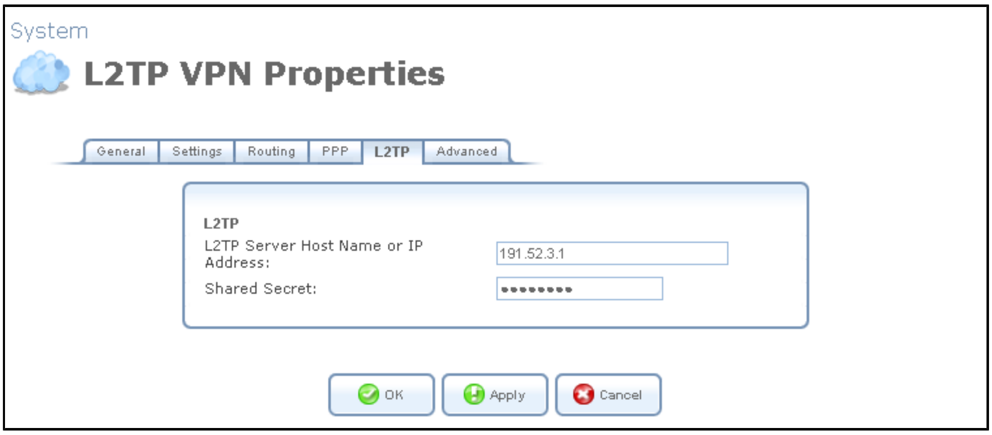


Figure 6.170 L2TP Configuration

6.4.9.3.6 Advanced

This sub-tab enables you to edit the advanced L2TP settings.

- **Internet Connection Firewall** Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

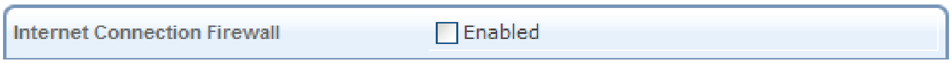


Figure 6.171 Internet Connection Firewall

6.4.10 Setting Up an L2TP Server

OpenRG can act as a Layer 2 Tunneling Protocol Server (L2TP Server), accepting L2TP client connection requests.

To set up a new L2TP Server, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears (see Figure 6.14).
2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').
3. Select the 'VPN Server' radio button and click 'Next'. The 'VPN Server' screen appears.

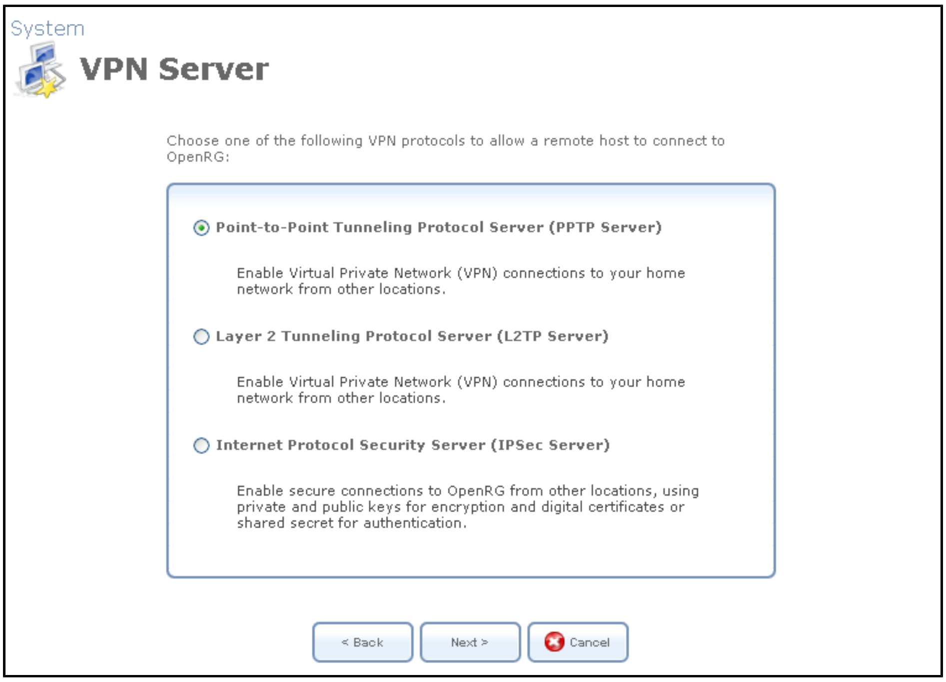


Figure 6.172 VPN Server

4. Select the 'Layer 2 Tunneling Protocol Server (L2TP Server)' radio button and click 'Next'. The 'Layer 2 Tunneling Protocol (L2TP)' screen appears.

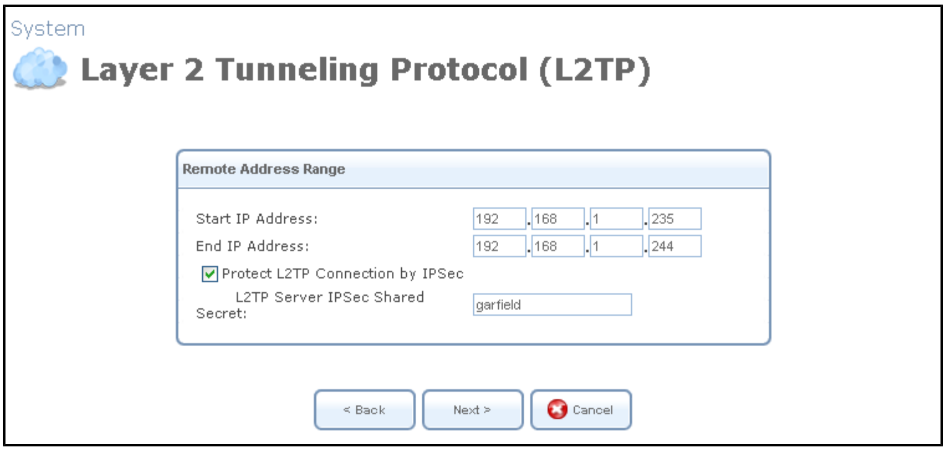


Figure 6.173 Layer 2 Tunneling Protocol (L2TP)

5. In this screen, perform the following:

   a. Specify the address range that OpenRG will reserve for remote users. You may use the default values as depicted in Figure 6.173.

   b. By default, the L2TP connection is protected by the IP Security (IPSec) protocol (the option is selected). However, if you wish to keep this setting, you must provide a string that will serve as the 'L2TP Server IPSec Shared Secret'. Alternatively, deselect this option to disable L2TP protection by IPSec.

6. Click 'Next'. The 'Connection Summary' screen appears (see Figure 6.174). Note the attention message alerting that there are no users with VPN permissions.

Figure 6.174 Connection Summary

7. Check the 'Edit the Connection' check box and click 'Finish'. The 'Layer 2 Tunneling Protocol Server (L2TP Server)' screen appears.

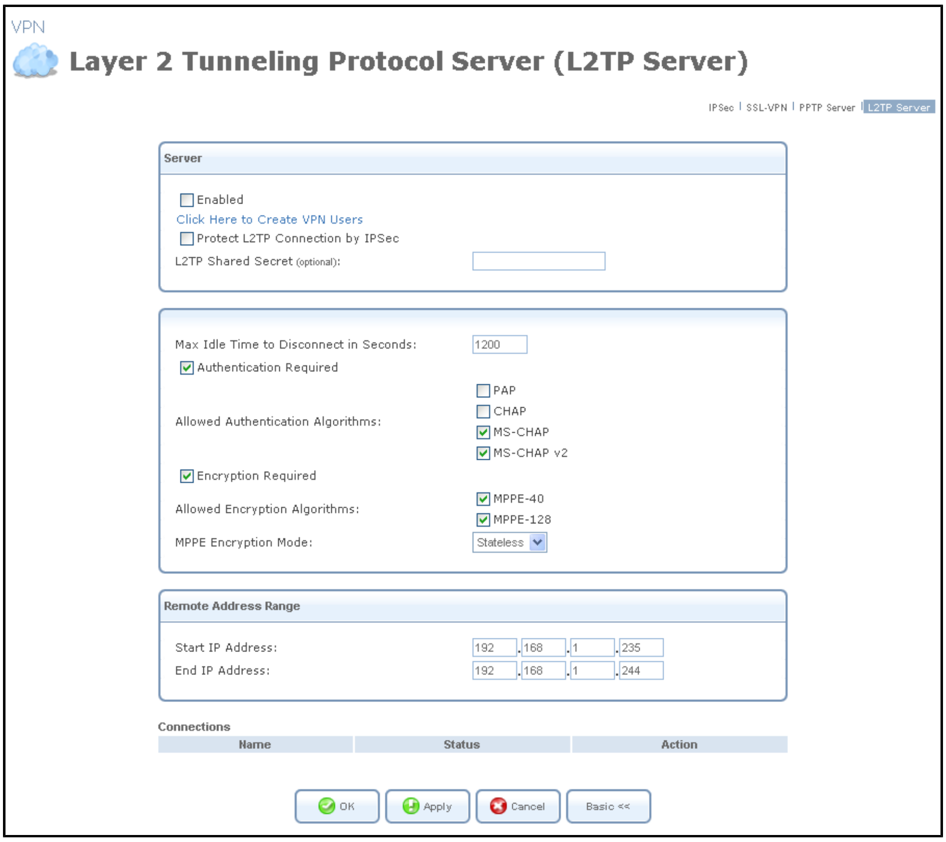


Figure 6.175 Advanced L2TP Server Parameters

8. Click the 'Click Here to Create VPN Users' link to define remote users that will be granted access to your home network. Refer to Section 6.3 to learn how to define and configure users.

9. Click 'OK' to save the settings.

The new L2TP Server will be added to the network connections list, and will be configurable like any connection. Unlike other connections, it is also accessible via the OpenRG's 'Advanced' screen. Note that the connection wizard automatically creates a default IPSec connection in order to protect the L2TP connection. To learn more, refer to Section 5.8.4.

To learn how to configure your L2TP and IPSec clients in order to connect to the L2TP server, refer to Section 5.8.4.3.

6.4.11 Setting Up a PPTP Connection

Point-to-Point Tunneling Protocol (PPTP) is a protocol developed by Microsoft targeted at creating VPN connections over the Internet. This enables remote users to access the gateway via any ISP that supports PPTP on its servers. PPTP encapsulates network traffic, encrypts content using Microsoft's Point-to-Point Encryption (MPPE) protocol that is based on RC4, and routes using the generic routing encapsulation (GRE) protocol. With OpenRG, PPTP is targeted at serving the following purposes:

1. Connecting OpenRG to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established by authenticating your user name and password.

2. Connecting OpenRG to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables secure transfer of data to another location over the Internet, by authenticating your username and password.

6.4.11.1 Creating a PPTP Connection

To create a new PPTP connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Internet Connection' radio button and click 'Next'. The 'Internet Connection' screen appears (see Figure 6.15).

3. Select the 'External Cable Modem' radio button (this option is for both internal and external cable modems) and click 'Next'. The 'Internet Cable Modem Connection' screen appears.

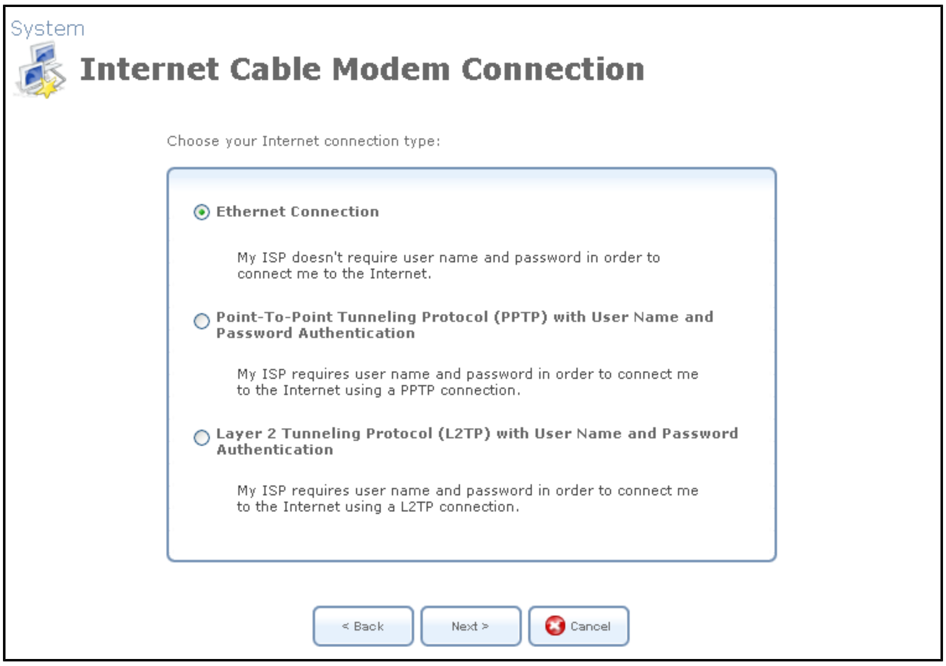


Figure 6.176 Internet Cable Modem Connection

4. Select the 'Point-To-Point Tunneling Protocol (PPTP) with User Name and Password Authentication' radio button and click Next. The 'Point-to-Point Tunneling Protocol (PPTP)' screen appears.

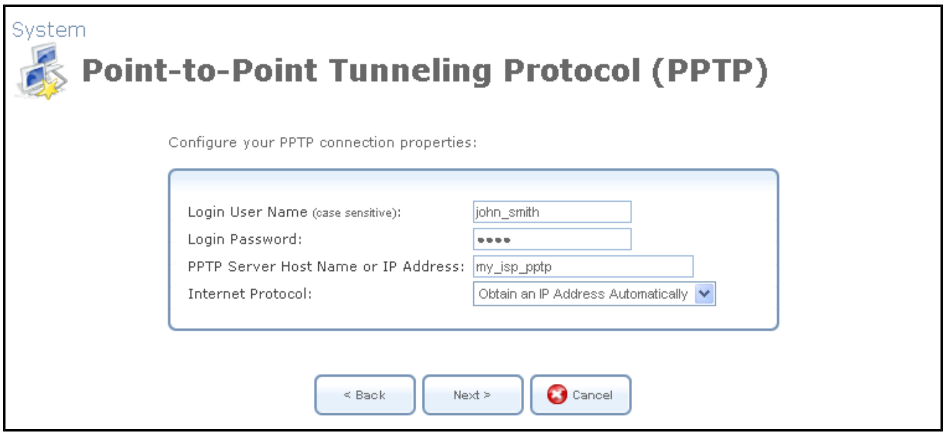


Figure 6.177 Point-to-Point Tunneling Protocol

5. Enter the username and password provided by your Internet Service Provider (ISP).
6. Enter the PPTP server's host name or IP address provided by your ISP.
7. Select whether to obtain an IP address automatically or specify one. This option is described in Section 6.4.11.3.2.
8. Click 'Next'. The 'Connection Summary' screen appears.

Figure 6.178 Connection Summary

9. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

10. Click 'Finish' to save the settings.

The new PPTP connection is added to the network connections list, and is configurable like any other connection.

6.4.11.2 Creating a PPTP VPN Connection

To create a new PPTP VPN connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').

3. Select the 'VPN Client or Point-To-Point' radio button, and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

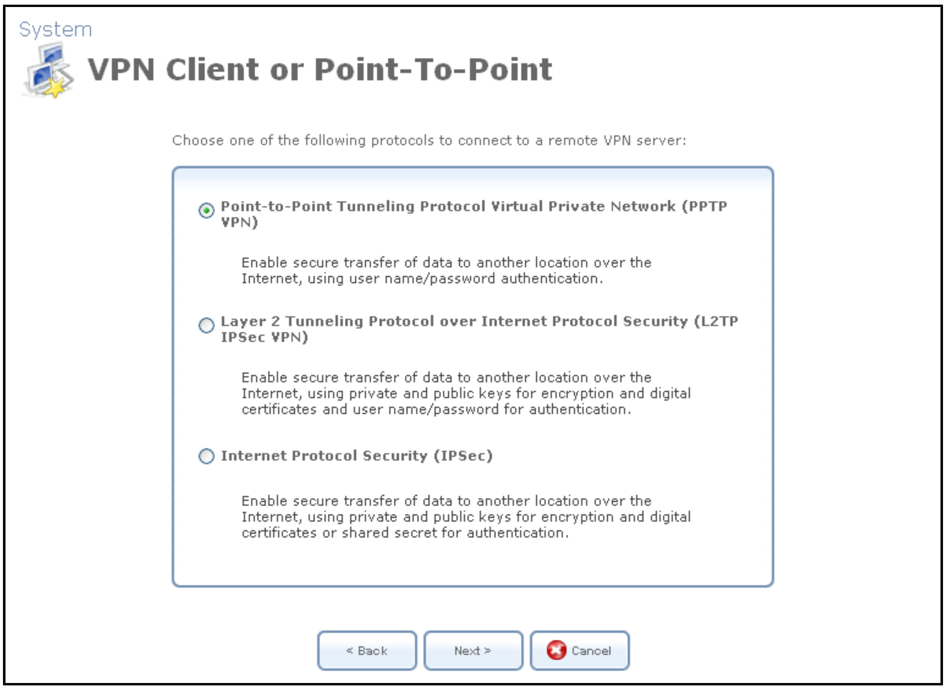


Figure 6.179 VPN Client or Point-To-Point

4. Select the 'Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)' radio button and click 'Next'. The 'Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)' screen appears.

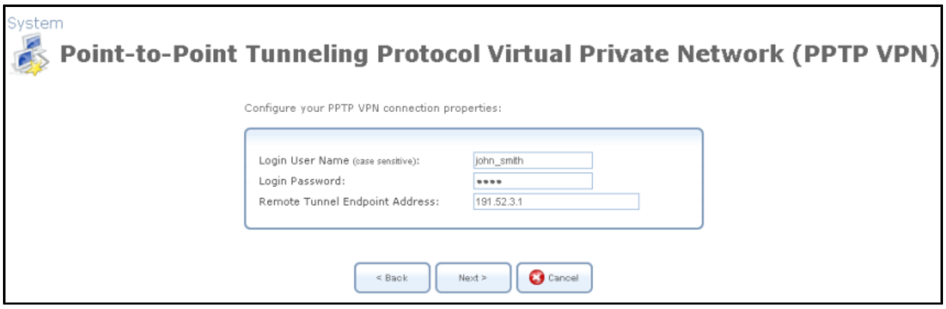


Figure 6.180 Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)

5. Enter the username and password provided by the administrator of the network you are trying to access.

6. Enter the remote tunnel endpoint address. This would be the IP address or domain name of the remote network computer, which serves as the tunnel's endpoint.

7. Click 'Next'. The 'Connection Summary' screen appears.

Figure 6.181 Connection Summary

8. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

9. Click 'Finish' to save the settings.

The new PPTP VPN connection is added to the network connections list, and is configurable like any other connection.

6.4.11.3 Viewing and Editing the Connection's Settings

To view and edit the PPTP connection settings, click the 'PPTP' link in the 'Network Connections' screen (see Figure 6.13). The 'PPTP Properties' screen appears.

Figure 6.182 PPTP Properties

6.4.11.3.1 General

This sub-tab enables you to view a detailed summary of the connection's settings. These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.11.3.2 Settings

This sub-tab enables you to edit the following PPTP connection settings:

General This section displays the connection's general parameters.

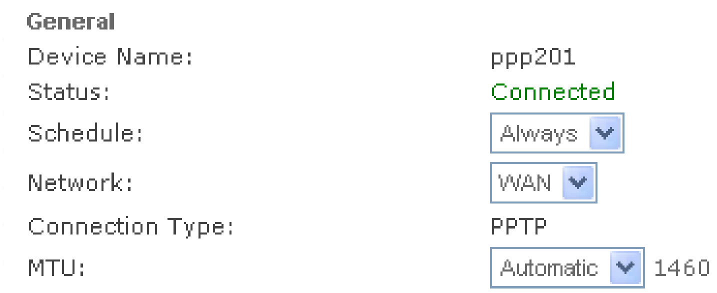


Figure 6.183 General PPTP Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- Obtain an IP Address Automatically

- Use the Following IP Address

Note that the screen refreshes to display relevant configuration settings according to your choice.

Obtain an IP Address Automatically Your connection is configured by default to obtain an IP automatically. You should change this configuration in case your service provider requires it. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead.

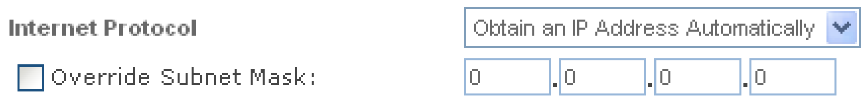


Figure 6.184 Internet Protocol – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

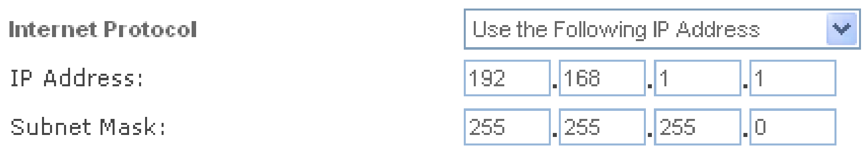


Figure 6.185 Internet Protocol – Static IP

DNS Server Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 6.186 DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

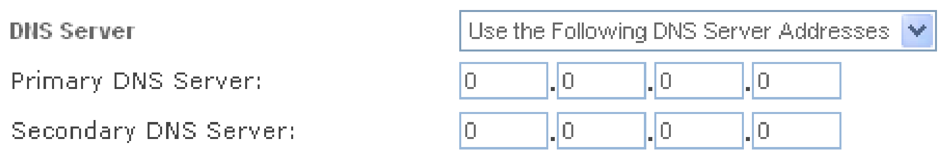


Figure 6.187 DNS Server – Static IP

To learn more about this feature, refer to Section 5.12.1.

6.4.11.3.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

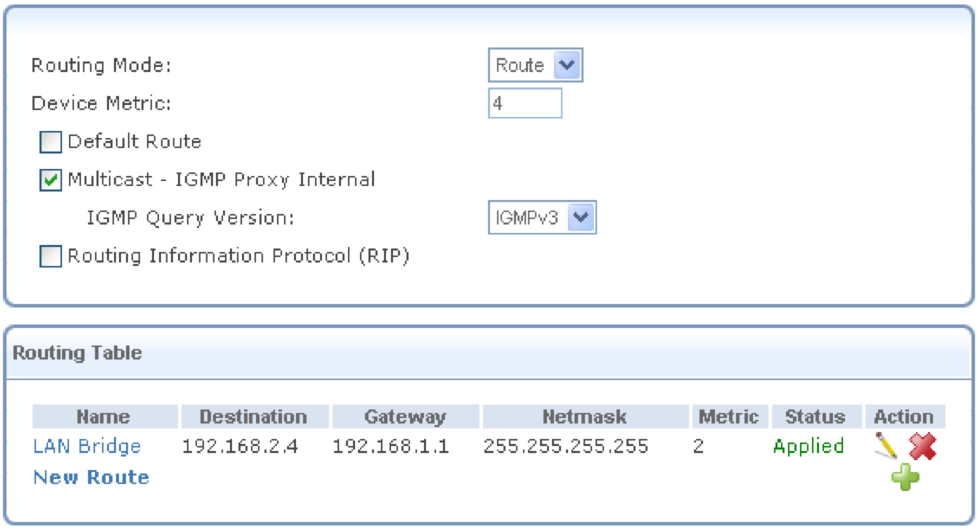


Figure 6.188 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
- **Send RIP messages**—select either 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.

Routing Table Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.
To learn more about this feature, refer to Section 6.6.

6.4.11.3.4 PPP

This sub-tab enables you to edit the following PPP settings.

PPP Point-to-Point Protocol (PPP) is the most popular method for transporting packets between the user and the Internet service provider. PPP supports authentication protocols such as PAP and CHAP, as well as other compression and encryption protocols.

PPP-on-Demand Use PPP on demand to initiate the point-to-point protocol session only when packets are actually sent over the Internet.

Time Between Reconnect Attempts Specify the duration between PPP reconnected attempts, as provided by your ISP.

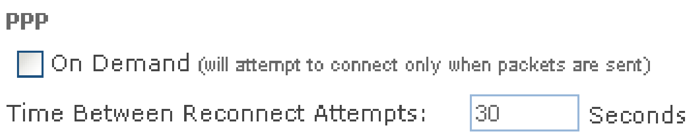


Figure 6.189 PPP Configuration

PPP Authentication Point-to-Point Protocol (PPP) currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2. This section allows you to select the authentication protocols your gateway may use when negotiating with a PPTP server. Select all the protocols if no information is available about the server's authentication protocols. Note that encryption is performed only if 'Microsoft CHAP', 'Microsoft CHAP version 2', or both are selected.

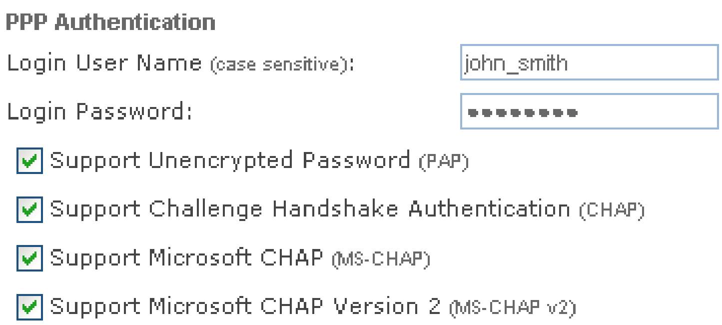


Figure 6.190 PPP Authentication

Login User Name As agreed with ISP.

Login Password As agreed with ISP.

Support Unencrypted Password (PAP) Password Authentication Protocol (PAP) is a simple, plain-text authentication scheme. The user name and password are requested by your networking peer in plain-text. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.

Support Challenge Handshake Authentication (CHAP) The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.

Support Microsoft CHAP Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.

Support Microsoft CHAP Version 2 Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.

PPP Encryption PPP supports encryption facilities to secure the data across the network connection. A wide variety of encryption methods may be negotiated, although typically only one method is used in each direction of the link. This section allows you to select the encryption methods your gateway may use when negotiating with a PPTP server. Select all the methods if no information is available about the server's encryption methods. Please note that PPP encryption can only be used with MS-CHAP or MS-CHAP-V2 authentication protocols.

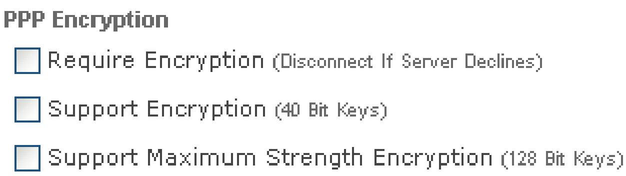


Figure 6.191 PPP Encryption

Require Encryption Select this check box to ensure that the PPP connection is encrypted.

Support Encryption (40 Bit Keys) Select this check box if your peer supports 40 bit encryption keys.

Support Maximum Strength Encryption (128 Bit Keys) Select this check box if your peer supports 128 bit encryption keys.

6.4.11.3.5 PPTP

This sub-tab enables you to edit the following PPTP settings.

PPTP Define your ISP's server parameters.

PPTP Server Host Name or IP Address Enter the connection's host name or IP address obtained from your ISP.

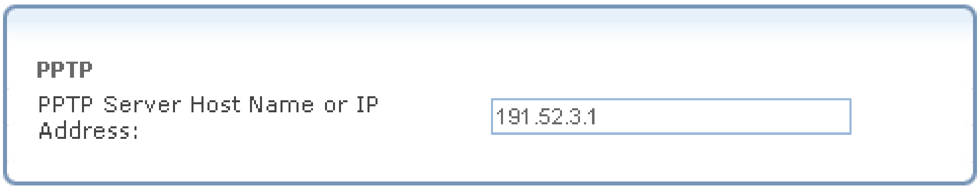


Figure 6.192 PPTP Configuration

6.4.11.3.6 Advanced

This sub-tab enables you to edit the advanced PPTP settings.

- **Internet Connection Firewall** Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

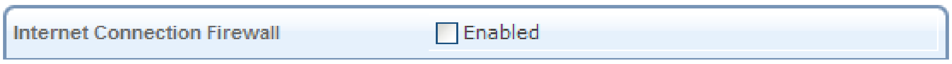


Figure 6.193 Internet Connection Firewall

6.4.12 Setting Up a PPTP Server

OpenRG can act as a Point-to-Point Tunneling Protocol (PPTP) Server, accepting PPTP client connection requests.

To set up a PPTP Server, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').

3. Select the 'VPN Server' radio button and click 'Next'. The 'VPN Server' screen appears.

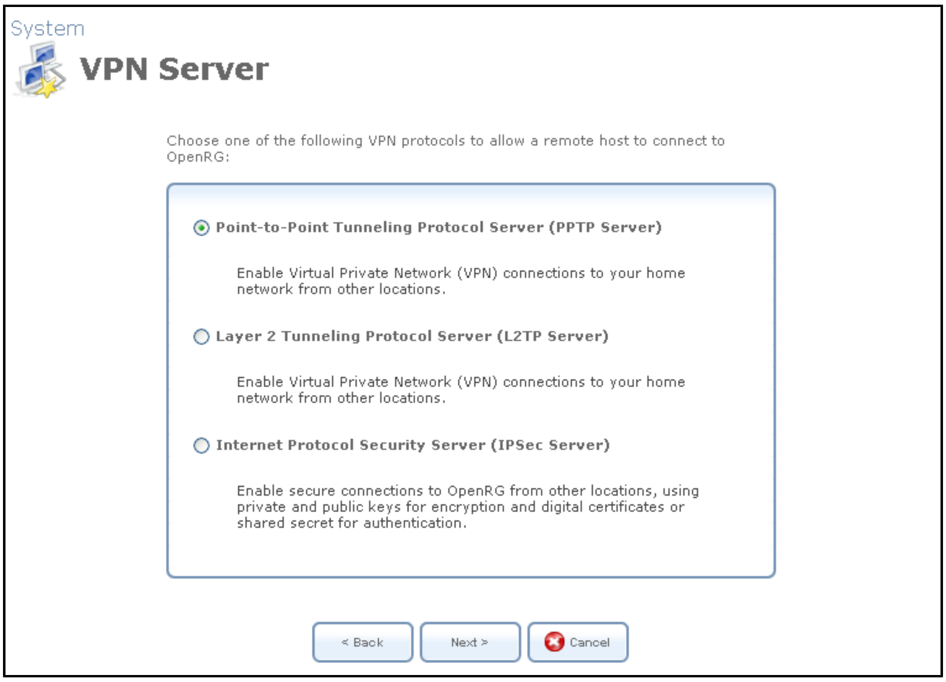


Figure 6.194 VPN Server

4. Select the 'Point-to-Point Tunneling Protocol Server (PPTP Server)' radio button and click 'Next'. The 'Point-to-Point Tunneling Protocol (PPTP)' screen appears.

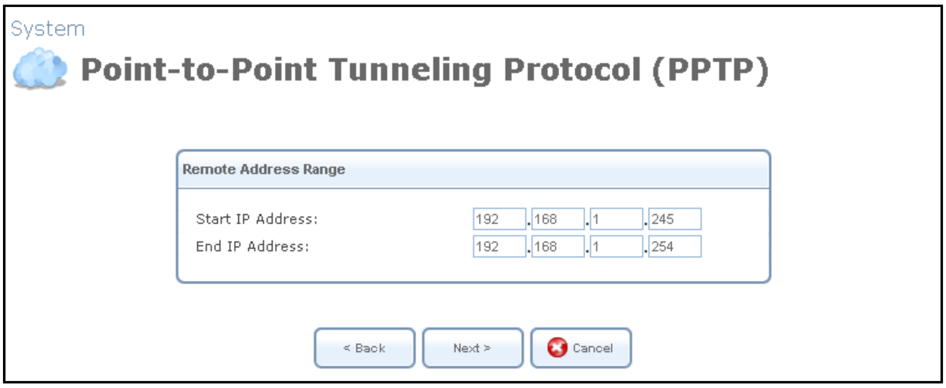


Figure 6.195 Point-to-Point Tunneling Protocol (PPTP)

5. Specify the address range that OpenRG will reserve for remote users. You may use the default values as depicted in Figure 6.195.

6. Click 'Next'. The 'Connection Summary' screen appears (see Figure 6.196). Note the attention message alerting that there are no users with VPN permissions.

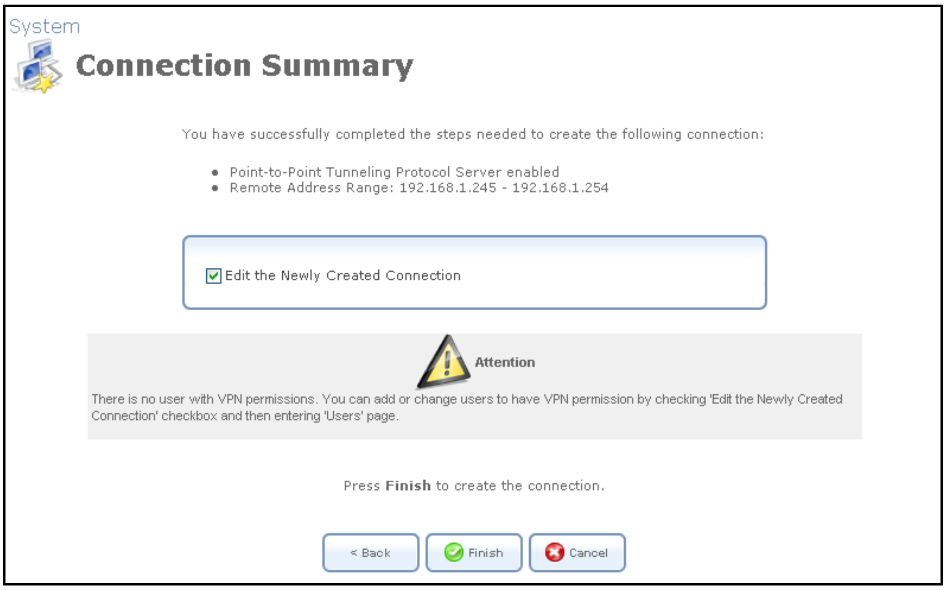


Figure 6.196 Connection Summary

7. Check the 'Edit the Newly Created Connection' check box and click 'Finish'. The 'Point-to-Point Tunneling Protocol Server (PPTP Server)' screen appears.

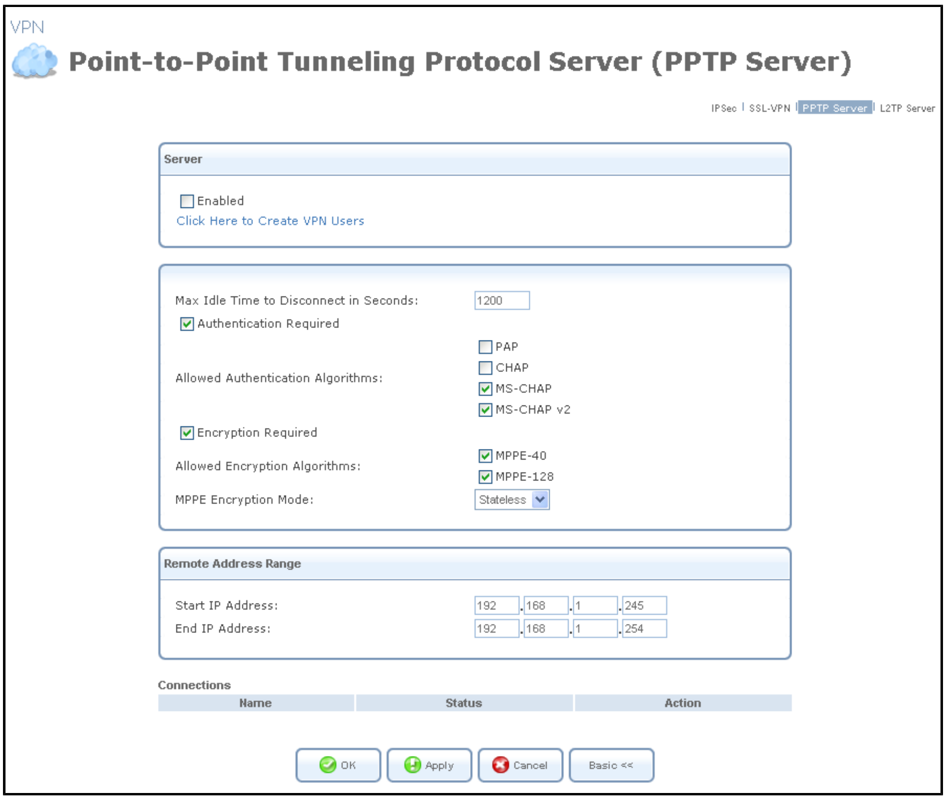


Figure 6.197 Advanced PPTP Server Parameters

8. Click the 'Click Here to Create VPN Users' link to define remote users that will be granted access to your home network. Refer to Section 6.3 to learn how to define and configure users.

9. Click 'OK' to save the settings.

The new PPTP Server will be added to the network connections list, and will be configurable like any connection. Unlike other connections, it is also accessible via the OpenRG's 'Advanced' screen. To learn more about the configuration of a PPTP server, refer to Section 5.8.3.

6.4.13 Setting Up an IPSec Connection

Internet Protocol Security (IPSec) is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies procedures for securing private information transmitted over public networks.

To set up an IPSec connection, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').

3. Select the 'VPN Client or Point-To-Point' radio button and click 'Next'. The 'VPN Client or Point-To-Point' screen appears.

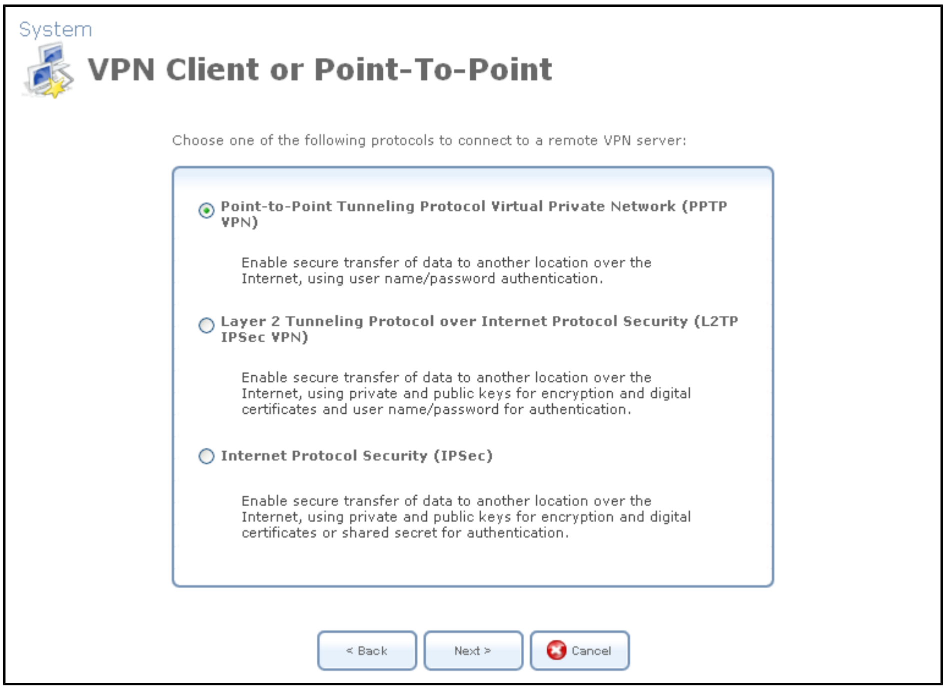


Figure 6.198 VPN Client or Point-To-Point

4. Select the 'Internet Protocol Security (IPSec)' radio button and click 'Next'. The 'Internet Protocol Security (IPSec)' screen appears.

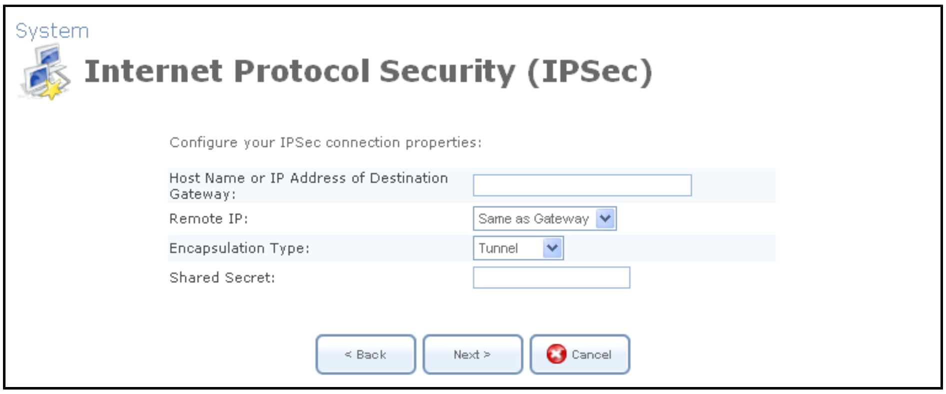


Figure 6.199 Internet Protocol Security (IPSec)

5. Enter the host name or IP address of the destination gateway.
6. Select a method for specifying the remote IP address, which serves as the tunnel's endpoint. Use "Same as Gateway" when connecting your LAN to a *remote gateway*. When connecting your LAN to a *remote network* (a group of computers beyond a gateway), use one of the remaining options. Also, use the *transport* encapsulation type in a gateway-to-gateway scenario only. Upon selection of an option, the screen refreshes providing you with the appropriate fields for entering the data.
   a. **Same as Gateway** – The default option that uses the gateway IP entered above. When selecting this option, you must also select the encapsulation type, tunnel or transport, from its drop-down menu.
   b. **IP Address –** The 'Remote IP Address' field appears. Specify the IP address.
   c. **IP Subnet** – The 'Remote Subnet IP Address' and 'Remote Subnet Mask' fields appear. Specify these parameters.
   d. **IP Range** – The 'From IP Address' and 'To IP Address' fields will appear. Specify the IP range.
7. Enter the IPSec shared secret, which is the encryption key jointly decided upon with the network you are trying to access.
8. Click 'Next'. The 'Connection Summary' screen appears.

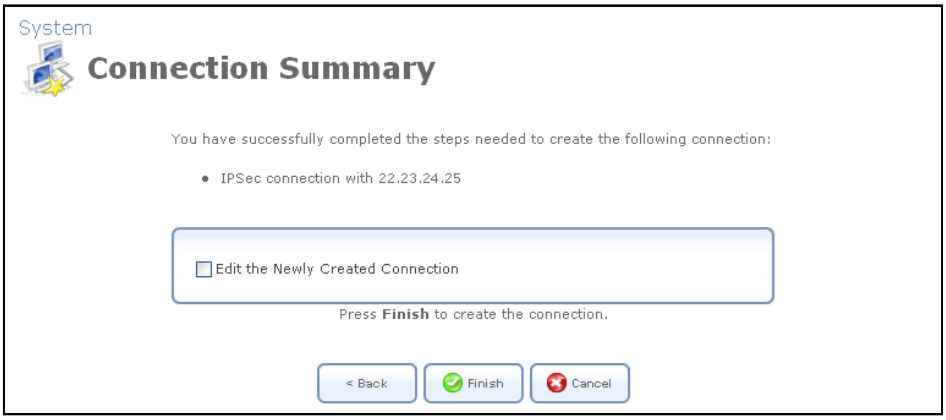


Figure 6.200 Connection Summary

9. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

10. Click 'Finish' to save the settings.

The new IPSec connection will be added to the network connections list, and will be configurable like any connection. Unlike other connections, it is also accessible via the OpenRG's 'Advanced' screen. To learn more about the configuration of an IPSec connection, refer to Section 5.8.1.

6.4.14 Setting Up an IPSec Server

To set up an Internet Protocol Security (IPSec) Server, perform the following:

1. Click the 'New Connection' link in the 'Network Connections' screen (see Figure 6.13). The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Connect to a Virtual Private Network over the Internet' radio button and click 'Next'. The 'Connect to a Virtual Private Network over the Internet' screen appears (see figure 'Connect to a Virtual Private Network over the Internet').

3. Select the 'VPN Server' radio button and click 'Next'. The 'VPN Server' screen appears.

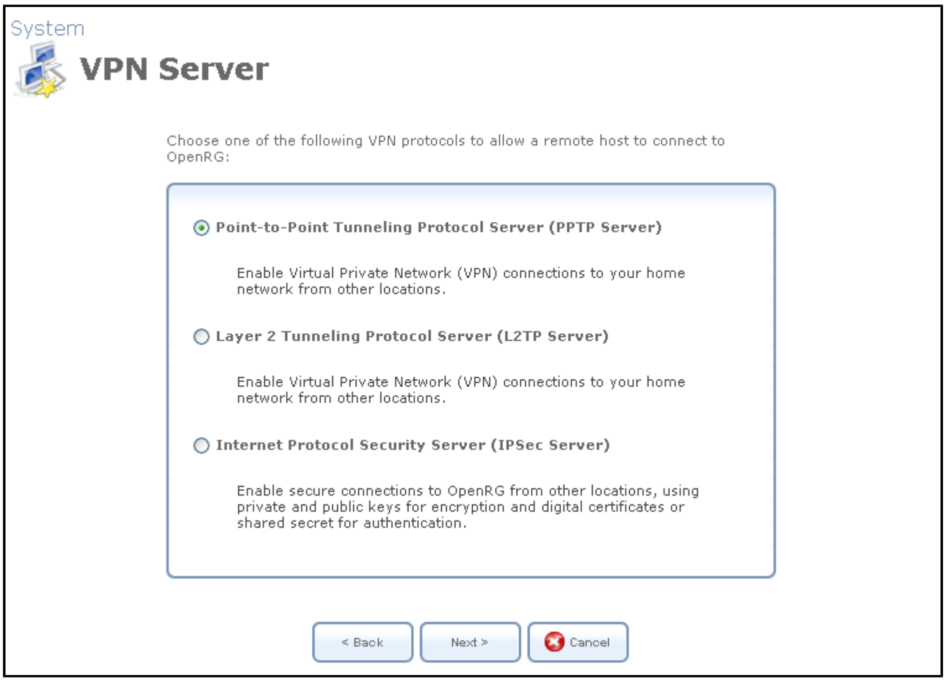


Figure 6.201 VPN Server

4. Select the 'Internet Protocol Security Server (IPSec Server)' radio button and click 'Next'. The 'Internet Protocol Security Server (IPSec Server)' screen appears.

Figure 6.202 Internet Protocol Security Server (IPSec Server)

5. Enter the IPSec shared secret, which is the encryption key jointly decided upon with the network you are trying to access.

6. Click 'Next'. The 'Connection Summary' screen appears.

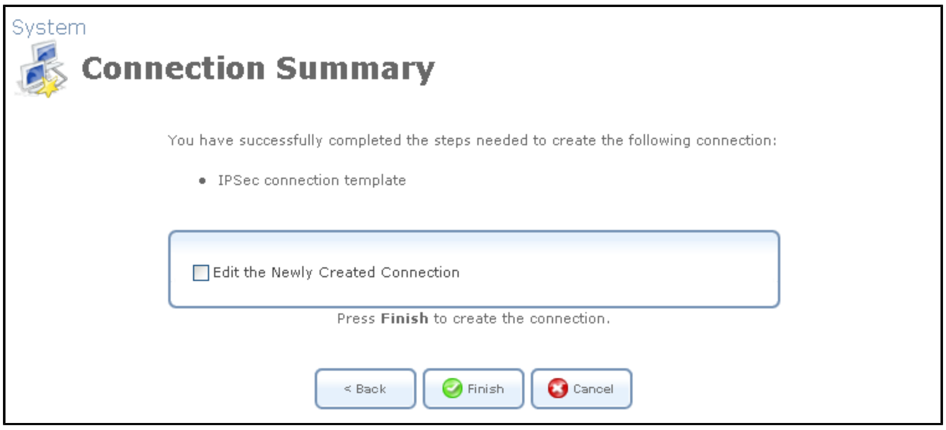


Figure 6.203 Connection Summary

7. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

8. Click 'Finish' to save the settings.

The new IPSec Server will be added to the network connections list, and will be configurable like any other connection. To learn more about the configuration of an IPSec server, refer to Section 5.8.1.

6.4.15 Setting up a WAN-LAN Bridge

A WAN-LAN bridge is a bridge over WAN and LAN devices. This way computers on the OpenRG LAN side can get IP addresses that are known on the WAN side.

6.4.15.1 Creating a WAN-LAN Bridge Connection

To create a new bridge or configure an existing one, perform the following:

1. In the 'Network Connections' screen under 'System' (see Figure 6.13), click the 'New Connection' link. The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears.

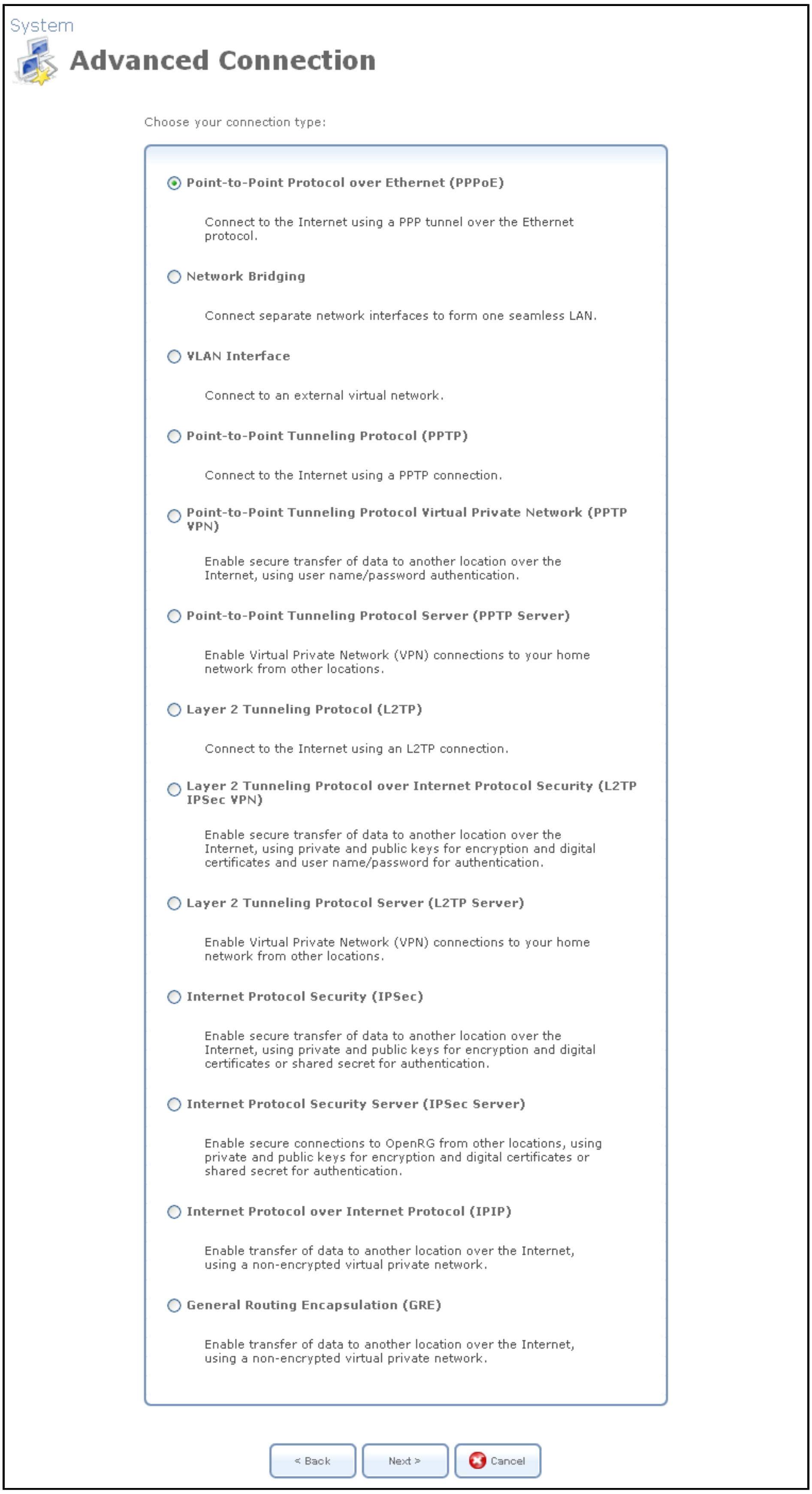


Figure 6.204 Advanced Connection Wizard

3. Select the 'Network Bridging' radio button and click 'Next'. The 'Bridge Options' screen appears.

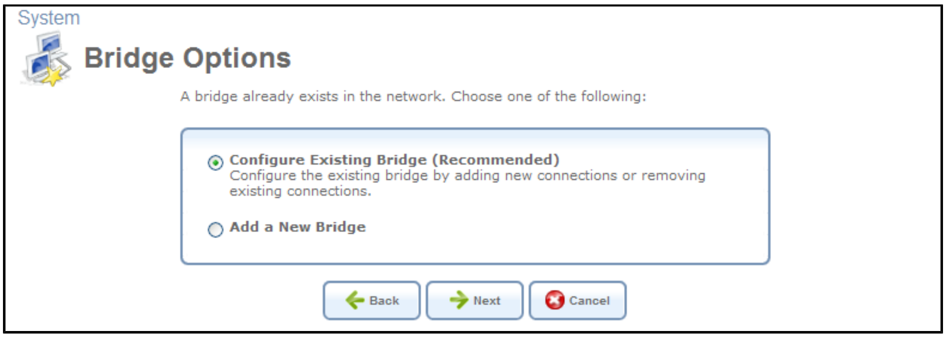


Figure 6.205 Bridge Options

4. Select whether to configure an existing bridge (this option will only appear if a bridge exists) or to add a new one:

   a. **Configure Existing Bridge** Select this option and click 'Next'. The 'Network Bridging' screen appears allowing you to add new connections to the bridge or remove existing ones, by selecting or deselecting their respective check boxes. For example, to create a WAN-LAN bridge, select the WAN connection's check box.

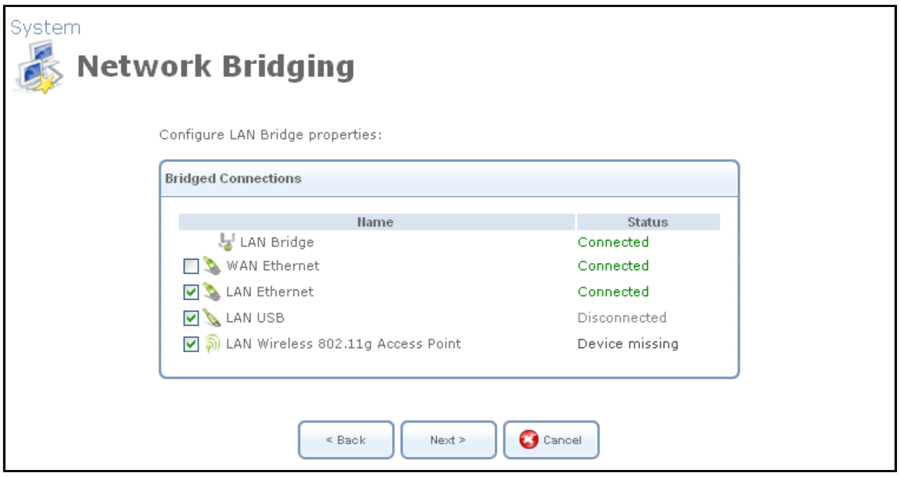


Figure 6.206 Network Bridging – Configure Existing Bridge

   b. **Add a New Bridge** Select this option and click 'Next'. A different 'Network Bridging' screen appears allowing you to add a bridge over the unbridged connections, by selecting their respective check boxes.

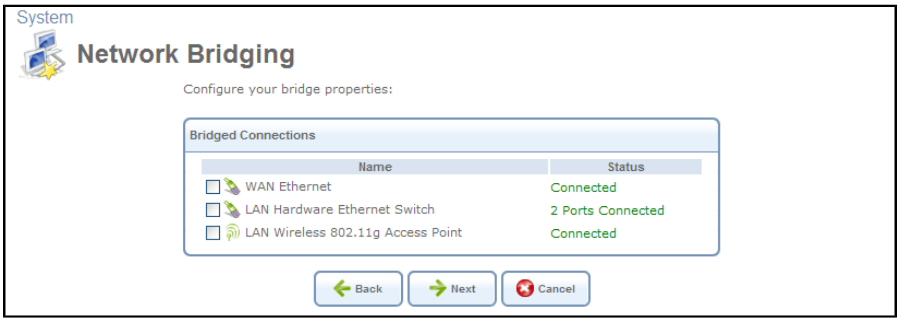


Figure 6.207 Network Bridging – Add a New Bridge

5. Click 'Next'. The 'Connection Summary' screen appears, corresponding to your changes.

Figure 6.208 Connection Summary – Configure Existing Bridge

6. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

7. Click 'Finish' to save the settings. The new bridge will be added to the network connections list, and it will be configurable like any other bridge.

The new bridge will be added to the network connections list, and it will be configurable like any other bridge.

> Note: Creating a WAN-LAN bridge disables OpenRG's DHCP server. This means that LAN hosts may only receive an IP address from a DHCP server on the WAN. If you configure a host with a static IP address from an alias subnet of the bridge (192.168.1.X), you will be able to access OpenRG but not the WAN, as NAT is not performed in the WAN-LAN bridge mode.

After creating a WAN-LAN bridge, you must also disable the IGMP Proxy on this connection. To do so, perform the following:

1. In the 'Network Connections' screen under 'System', click the 'LAN Bridge' link. The 'LAN Bridge Properties' screen appears.

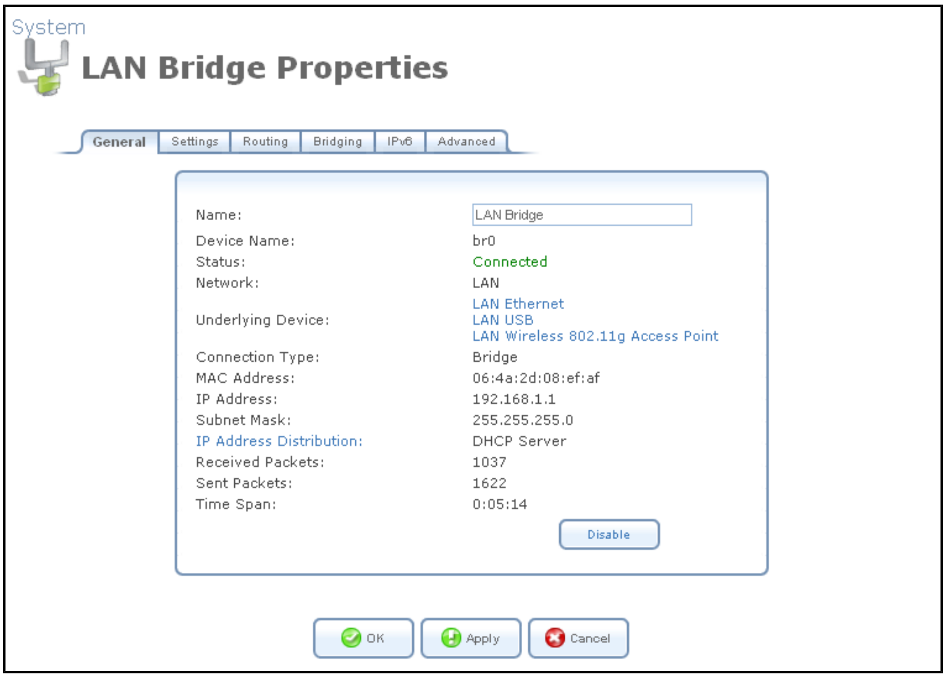


Figure 6.209 LAN Bridge Properties

2. Select the 'Routing' sub-tab, and disable the 'Multicast - IGMP Proxy Default' option (to learn more about this option, refer to Section 6.4.15.3.3).

3. Click 'OK' to save the settings.

6.4.15.2 Enabling the Hybrid Bridging Mode

OpenRG enables you to bridge certain bandwidth-consuming and traffic-sensitive LAN hosts, such as IPTV Set Top Boxes, directly to the WAN. Such a network connection scheme does not interfere with OpenRG's routing mode, in which all traffic usually passes through the NAT, and is checked by the firewall. These two modes can work simultaneously, if you have two bridges under OpenRG's LAN network device:

LAN bridge Receives its IP address from OpenRG's DHCP server. The traffic passing through the LAN on its way to the WAN is inspected by OpenRG's firewall, and assigned a public address by the NAT.

WAN-LAN bridge Receives its IP address from the WAN DHCP server, thereby enabling direct communication with the WAN.
OpenRG based on Linux 2.6 supports direct communication between devices placed under the two bridges. For example, if you connect your IPTV Set Top Box with a Personal Video Recorder (PVR) to OpenRG's WAN-LAN bridge, you will be able to access the content recorded on the PVR from any home computer connected to OpenRG's LAN.

This network configuration is called *Hybrid Bridging*. OpenRG detects LAN hosts that should be bridged to the WAN according to their MAC address or a specific DHCP option (either **Vendor Class ID**, **Client ID** or **User Class ID**). Once detected, these LAN hosts are placed

under the WAN-LAN bridge, which you must add and configure for the hybrid bridging mode beforehand.

To add the WAN-LAN bridge, follow the Connection Wizard steps described in Section 6.4.15.1. In the final step, check the 'Edit the Newly Created Connection' check box, and click 'Finish'. The 'Bridge Properties' screen appears.

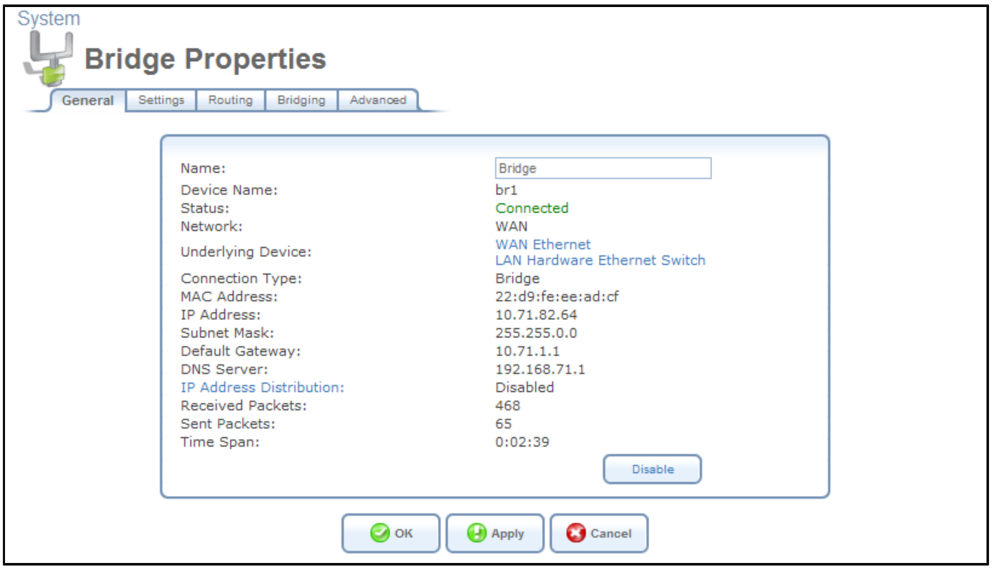


Figure 6.210 Bridge Properties

To configure the WAN-LAN bridge for the hybrid bridging mode, perform the following:

1. In the 'Bridge Properties' screen, click the 'Routing' tab. The following screen appears.

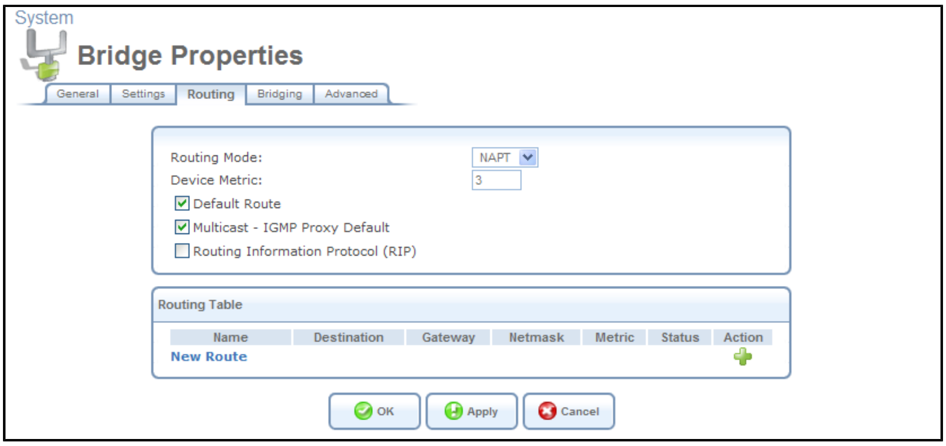


Figure 6.211 WAN-LAN Bridge Routing Settings

2. From the 'Routing Mode' drop-down menu, select 'Route' and click 'Apply'. The following warning screen appears.

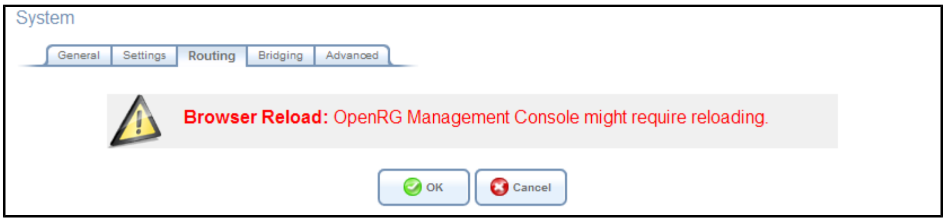


Figure 6.212 Browser Reload Warning Message

3. Click 'OK'. The page refreshes while saving the new settings, and returns to the previous screen.

4. Click the 'Bridging' tab. The following screen appears.

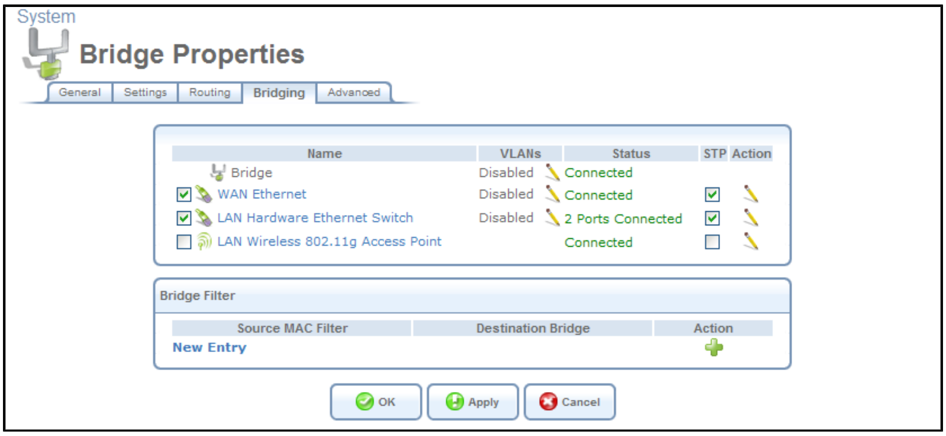


Figure 6.213 WAN-LAN Bridging Settings

5. In the 'Bridge Filter' section, click the 'New Entry' link. The following screen appears.

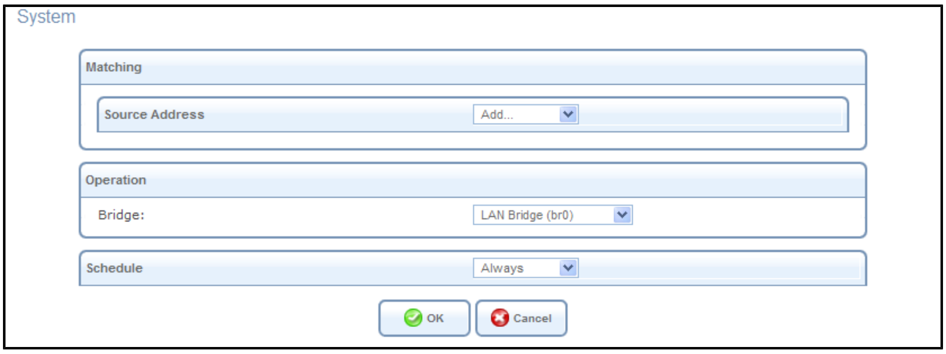


Figure 6.214 Bridge Filter Settings

6. From the drop-down menu in the 'Operation' section, select the WAN-LAN bridge. If not renamed, its default entry appears as "Bridge (br1)".

7. From the 'Source Address' drop-down menu, select 'User Defined'. The 'Edit Network Object' screen appears.

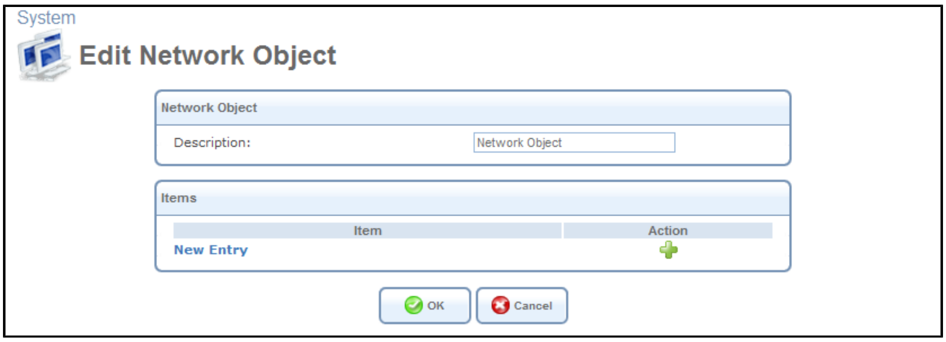


Figure 6.215 Edit Network Object

8. Click the 'New Entry' link. The 'Edit Item' screen appears.

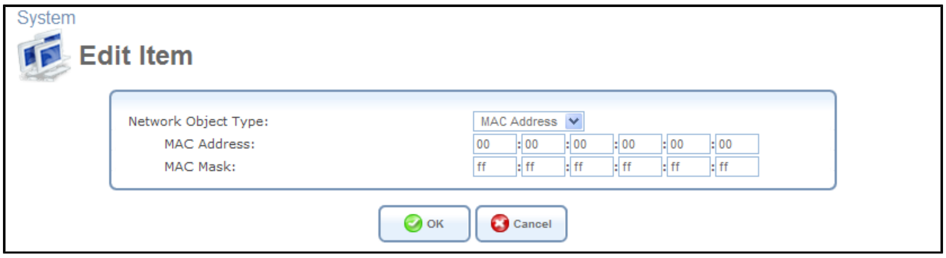


Figure 6.216 Edit Item – MAC Address

This screen enables you to create a traffic filtering rule, which enables direct packet flow between the WAN and the LAN host that will be placed under the WAN-LAN bridge. This filtering rule can be based on either a LAN host's MAC address or one of its DHCP options mentioned earlier.

9. If you wish to base this rule on the MAC address, enter the MAC address and the MAC mask in their respective fields. Otherwise, perform the following:

   a. From the 'Network Object Type' drop-down menu, select 'DHCP Option'. The screen refreshes, changing to the following.

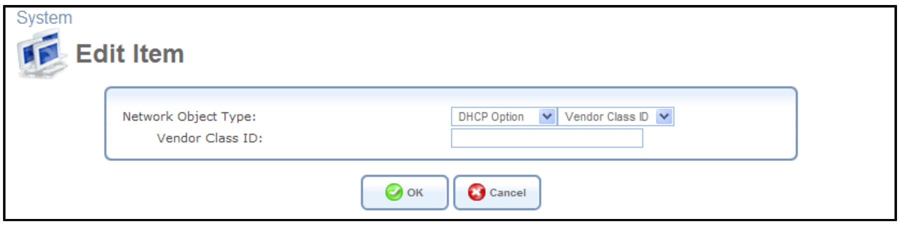


Figure 6.217 Edit Item – DHCP Options

   b. From the designated drop-down menu, select one of the DHCP options. The field below changes accordingly.

   c. Enter a relevant value for the DHCP option (should be supplied by your service provider).

10. Click 'OK' to save the settings.

6.4.15.3 Viewing and Editing the Connection's Settings

To view and edit the WAN-LAN bridge connection settings, click the 'Bridge' link in the 'Network Connections' screen (see Figure 6.13). The 'Bridge Properties' screen appears.

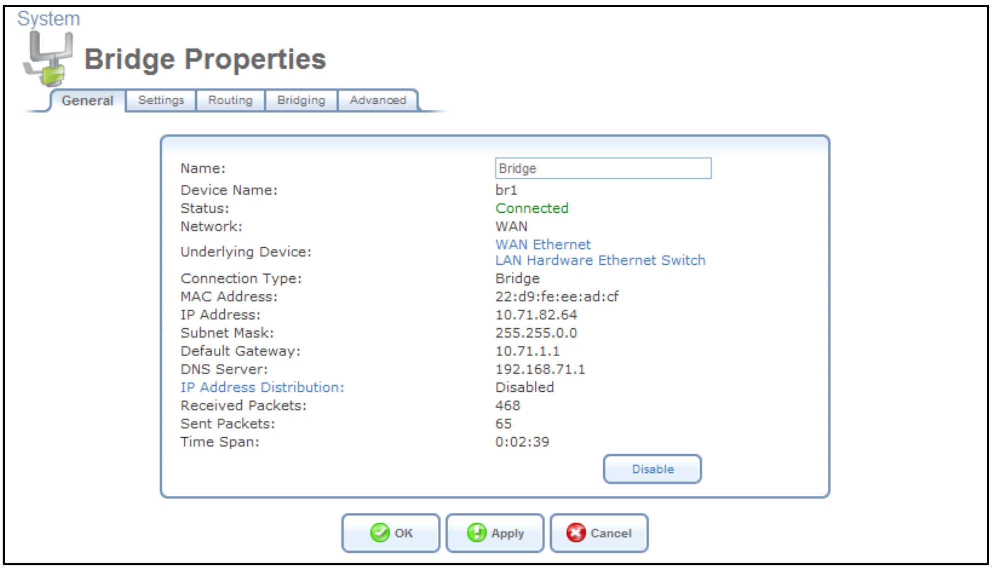


Figure 6.218 Bridge Properties

6.4.15.3.1 General

This sub-tab enables you to view a detailed summary of the WAN-LAN bridge connection settings (see Figure 6.13). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.15.3.2 Settings

This sub-tab enables you to edit the following WAN-LAN bridge connection settings.

General This section displays the connection's general parameters.

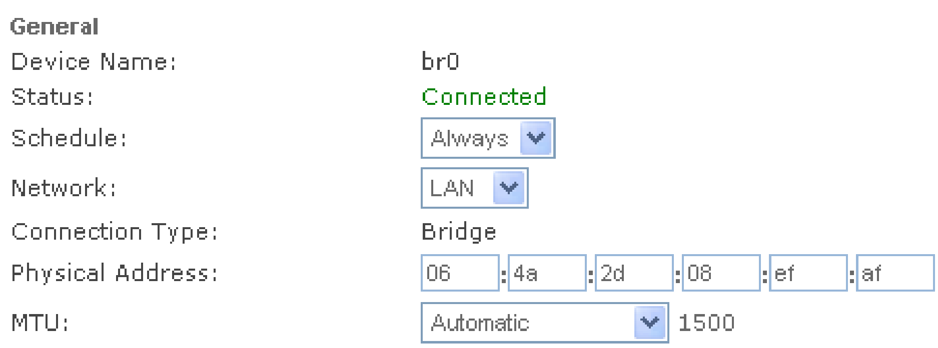


Figure 6.219 General Bridge Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

Clone My MAC Address Press this button to copy your PC's current MAC address to the board.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen will refresh to display relevant configuration settings according to your choice.

No IP Address Select 'No IP Address' if you require that your gateway have no IP address. This can be useful if you are working in an environment where you are not connected to other networks, such as the Internet.

Figure 6.220 Internet Protocol – No IP Address

Obtain an IP Address Automatically Your connection is configured by default to act as a DHCP client. You should keep this configuration in case your service provider supports DHCP, or if you are connecting using a dynamic IP address. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead. You can click the 'Release' button to release the current leased IP address. Once

the address has been released, the button text changes to 'Renew'. Use the 'Renew' button to renew the leased IP address.

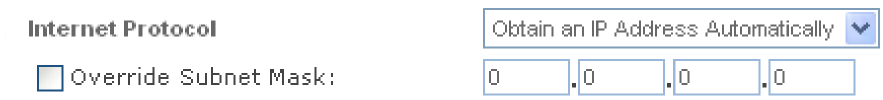


Figure 6.221 Internet Protocol Settings – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

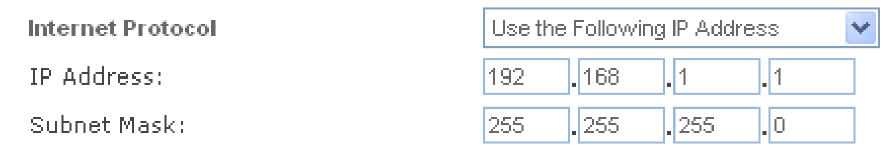


Figure 6.222 Internet Protocol – Static IP

DNS Server Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses. You can configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP. To configure the connection to automatically obtain a DNS server address, select 'Obtain DNS Server Address Automatically' from the 'DNS Server' drop down menu.

Figure 6.223 DNS Server – Automatic IP

To manually configure DNS server addresses, select 'Use the Following DNS Server Addresses' from the 'DNS Server' drop down menu (see figure 'DNS Server -- Static IP'). Specify up to two different DNS server address, one primary, another secondary.

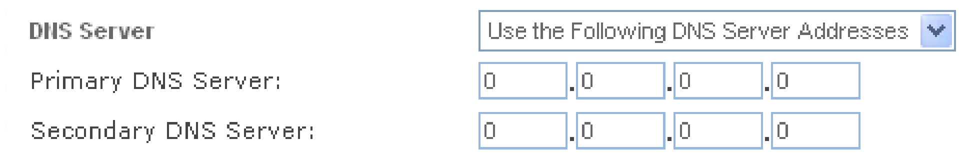


Figure 6.224 DNS Server – Static IP

To learn more about this feature, refer to Section 5.12.1.

IP Address Distribution In general, the 'IP Address Distribution' section enables you to configure the DHCP server parameters. However, in the WAN-LAN bridge configuration, the DHCP server must be disabled.

6.4.15.3.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts

how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

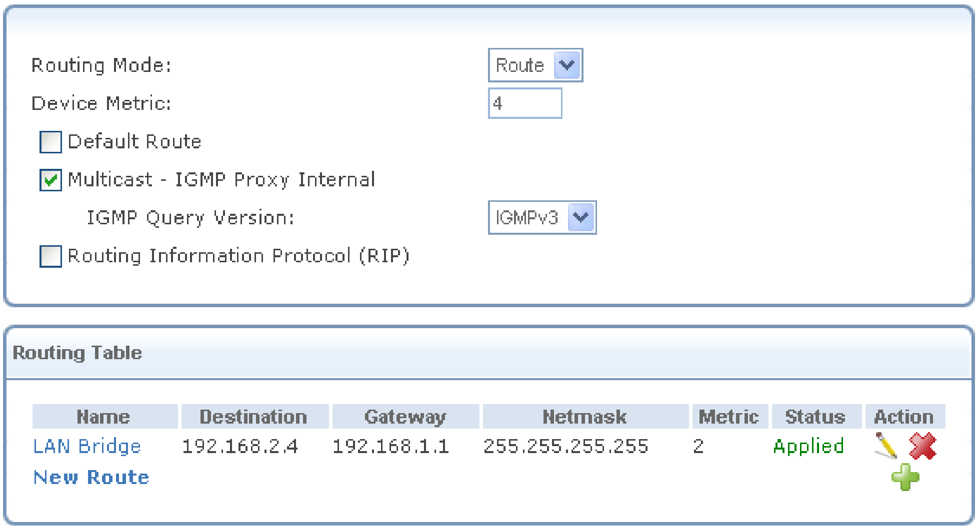


Figure 6.225 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

> **Route** Use route mode if you want your gateway to function as a router between two networks.
>
> **NAPT** Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

> **IGMP Query Version** OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
- **Send RIP messages**—select either 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.

Routing Table Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.
To learn more about this feature, refer to Section 6.6.

6.4.15.3.4 Bridging

This sub-tab enables you to specify the devices that you would like to join under the network bridge.

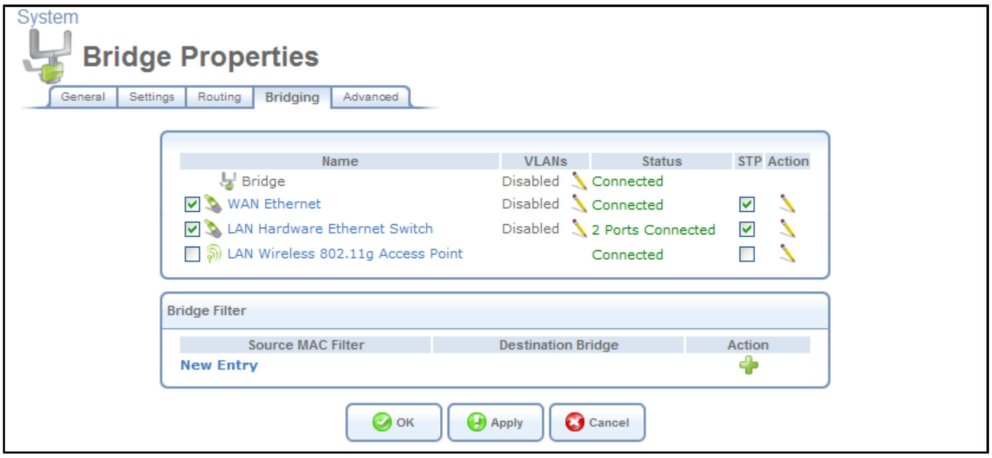


Figure 6.226 Bridge Settings

If you wish to assign the network connections to specific virtual LANS (VLANs), click the action icon under the 'VLANs' column.

> Note: If you would like to logically partition your Ethernet-based network, you can set up a VLAN bridge as described in Section 6.4.16.4.

Select the 'STP' check box to enable the Spanning Tree Protocol on the device. Use this feature to ensure that there are no loops in your network configuration, especially in case your network consists of multiple switches, or other bridges apart from those created by the gateway. By blocking redundant connections, STP enables a single data path between LAN hosts. If a device or a link failure causes this path to become unusable, STP will enable an alternative path. Note that OpenRG also supports the Rapid Spanning Tree Protocol (RSTP), which provides a faster response to changes in your local network topology than STP.

6.4.15.3.5 IPv6

This subtab enables you to define new IPv6 addresses for the current connection, by clicking the 'New Unicast Address' link. Note that this sub-tab appears only if the IPv6 feature is enabled on the gateway. For more information, refer to Section 6.6.2.

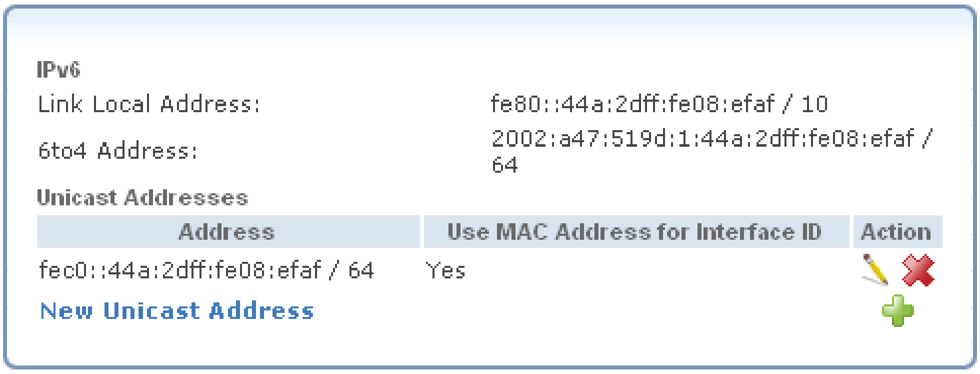


Figure 6.227 IPv6 Settings

6.4.15.3.6 Advanced

This sub-tab enables you to edit the connection's advanced settings.

- **Internet Connection Firewall** Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

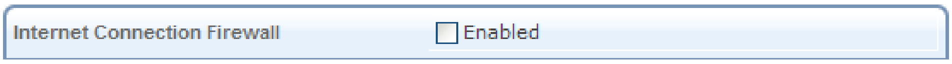


Figure 6.228 Internet Connection Firewall

- **Additional IP Addresses** You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://openrg.home.

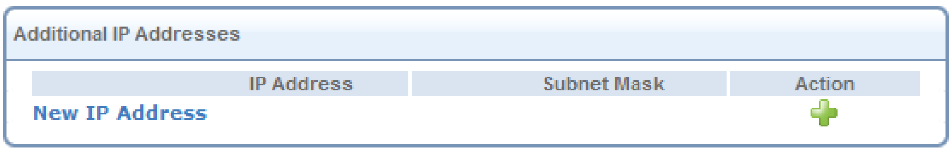


Figure 6.229 Additional IP Addresses

6.4.16 Setting Up a VLAN Interface

A Virtual LAN (VLAN)interface enables you to group workstations together into one broadcast domain, even if they are not located on the same LAN segment. OpenRG allows you to create virtual Ethernet-based networks according to the IEEE 802.1Q standard. If you would like your VLANs to communicate with the same network node without communicating with each other, use OpenRG's VLAN bridging capability as described in Section 6.4.16.4.

6.4.16.1 Creating a VLAN Interface

To create a new VLAN interface, perform the following:

1. In the 'Network Connections' screen under 'System' (see Figure 6.13), click the 'New Connection' link. The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears.

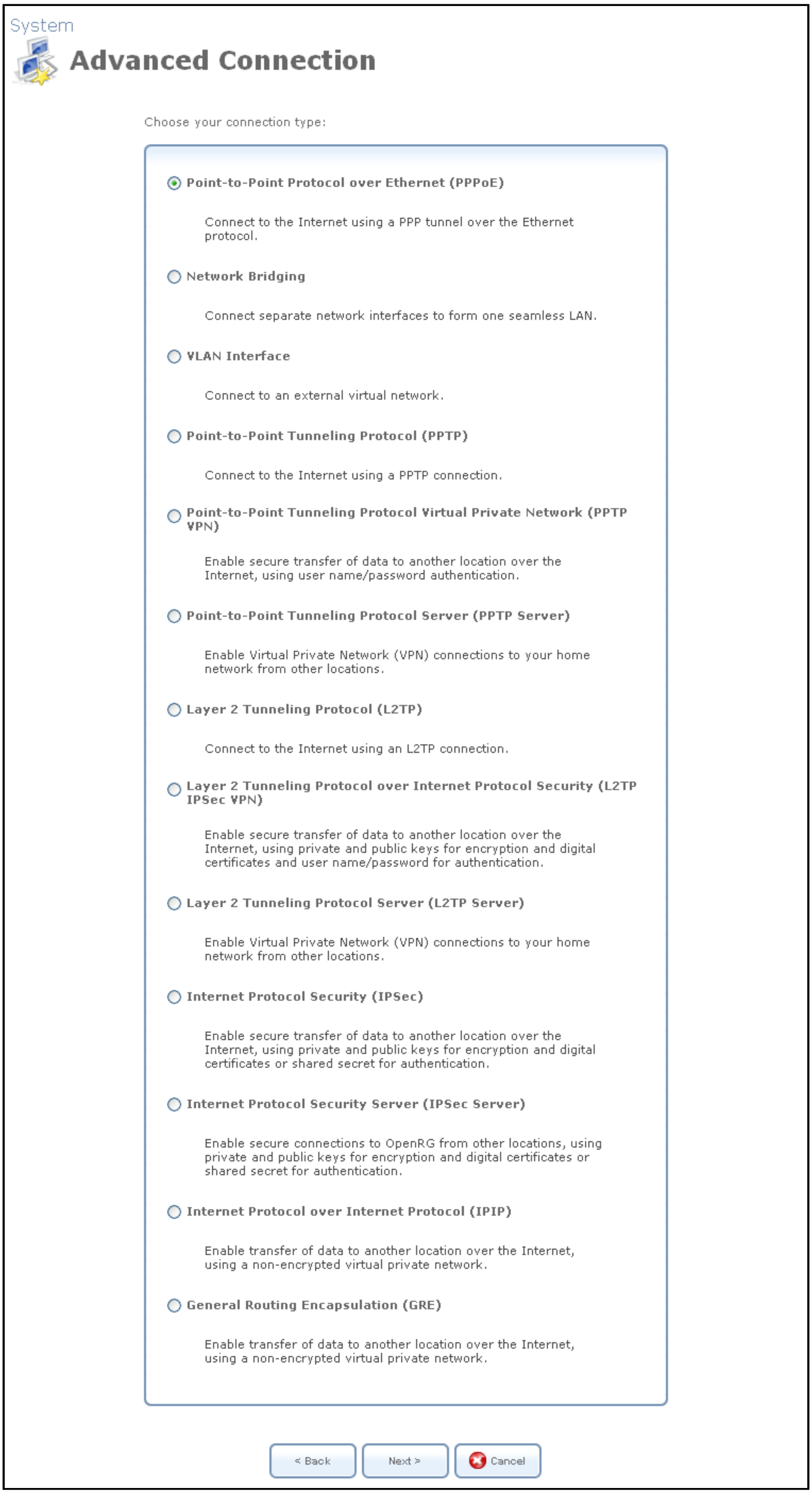


Figure 6.230 Advanced Connection Wizard

3. Select the 'VLAN Interface' radio button and click 'Next'. The 'VLAN Interface' screen appears.

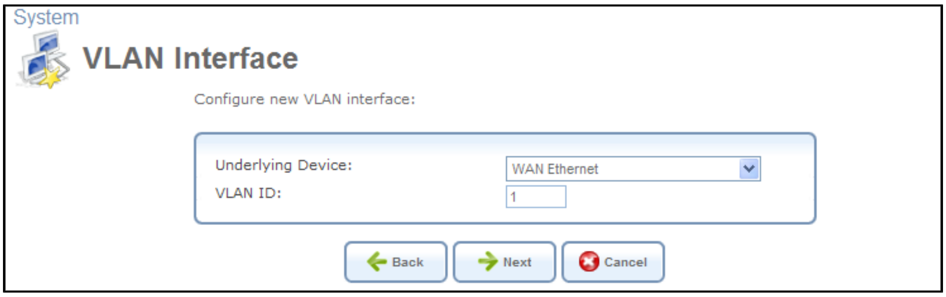


Figure 6.231 VLAN Interface

Note: By default, all of the gateway's physical LAN devices are enslaved by OpenRG's LAN bridge. A VLAN cannot be created over an enslaved network device. Therefore, remove a device from the bridge prior to creating a VLAN over it. To learn how to do so, refer to Section 6.4.5.1.

4. Select the underlying device for this interface. The drop-down menu will display OpenRG's Ethernet connections.

5. Enter a value that will serve as the VLAN ID, and click 'Next'. If you choose to create the VLAN over the LAN bridge, the following screen appears.

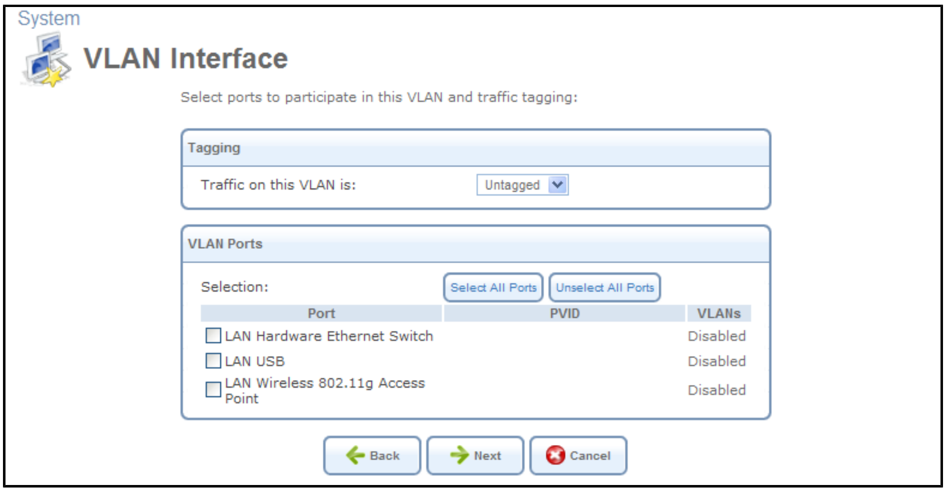


Figure 6.232 VLAN over LAN Bridge

Tagging This feature enables you to select whether to add a *tag header* (a 32-bit label serving as a VLAN ID) to the frames transferred over the VLAN. When the 'Untagged' option is selected, the VLAN is determined based on other information, such as the ID of a port on which the data arrived (PVID). Select the relevant setting from the designated drop-down menu. If the created virtual network is intended for VLAN-unaware hosts, it is recommended that you select the 'Untagged' option.

VLAN Ports You can select the LAN bridge ports on which you would like to enable the VLAN. To enable the VLAN on a specific device port, select its check box. You can also select or deselect all of the ports by clicking the corresponding buttons.

6. After setting the VLAN parameters, click 'Next'. The 'Connection Summary' screen appears.

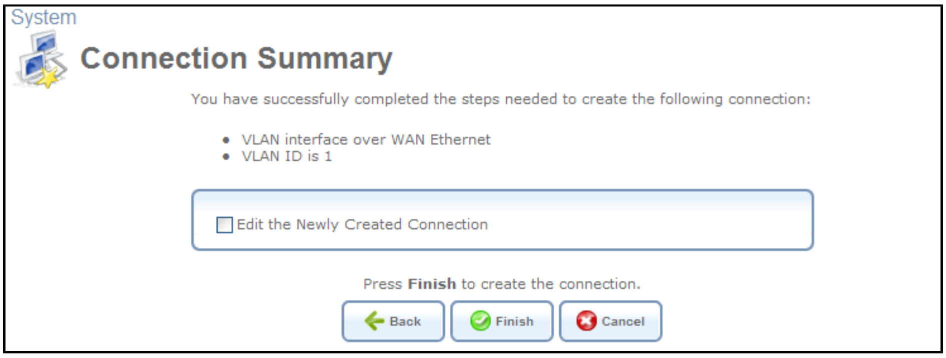


Figure 6.233 Connection Summary

7. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

8. Click 'Finish' to save the settings.

The new VLAN interface will be added to the network connections list, and will be configurable like any other connection.

6.4.16.2 Viewing and Editing the VLAN Interface Settings

To view and edit the VLAN interface settings, click its link. For example, click the 'WAN Ethernet 2' link in the 'Network Connections' screen. The 'WAN Ethernet 2 Properties' screen appears.

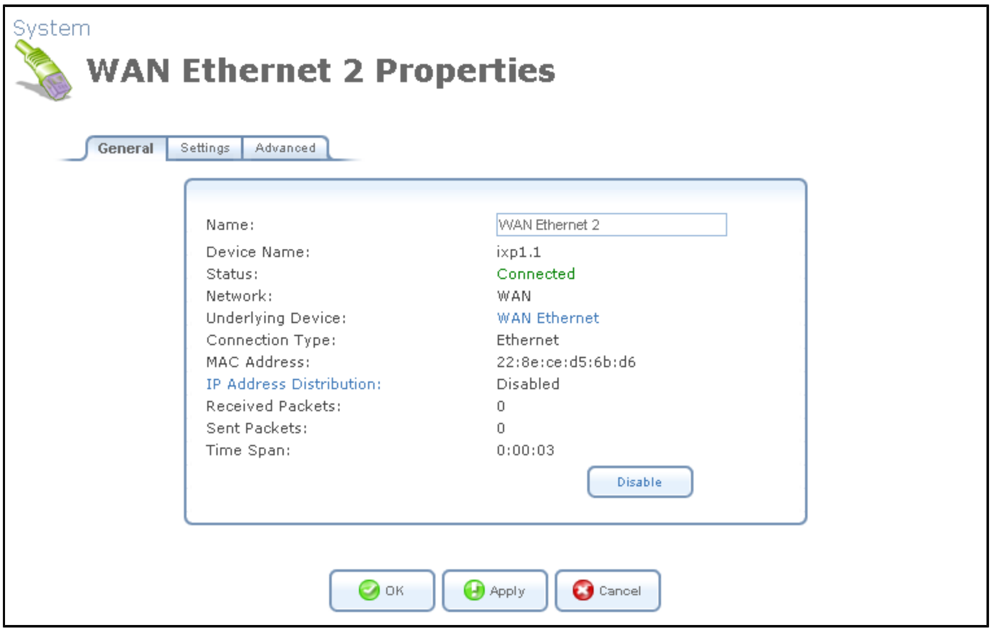


Figure 6.234 WAN Ethernet 2 Properties

6.4.16.2.1 General

This sub-tab enables you to view a detailed summary of the VLAN interface settings (see Figure 6.234). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.16.2.2 Settings

This sub-tab enables you to edit the following VLAN interface settings.

General This section displays the connection's general parameters.

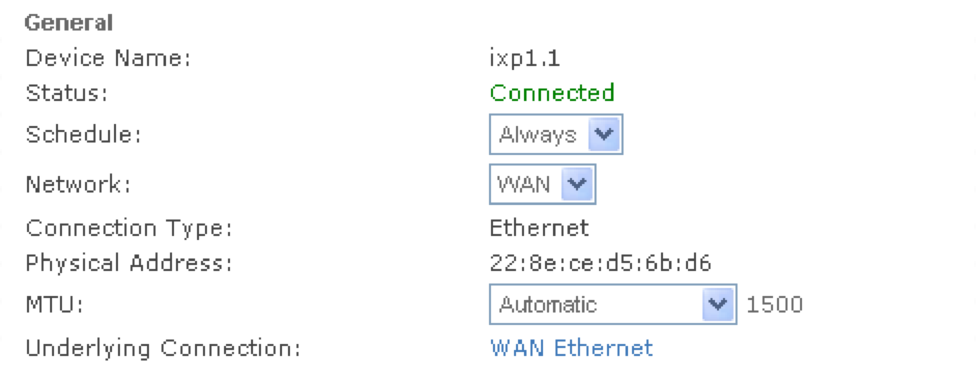


Figure 6.235 General VLAN Interface Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

Physical Address The physical address of the network interface for your network. Some interfaces allow you to change this address.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Underlying Connection The Ethernet device over which the connection is implemented.

Internet Protocol Select one of the following Internet protocol options from the 'Internet Protocol' drop-down menu:

- No IP Address
- Obtain an IP Address Automatically
- Use the Following IP Address

Note that the screen will refresh to display relevant configuration settings according to your choice.

No IP Address Select 'No IP Address' if you require that your gateway have no IP address. This can be useful if you are working in an environment where you are not connected to other networks, such as the Internet.

Figure 6.236 Internet Protocol – No IP Address

Obtain an IP Address Automatically Your connection is configured by default to act as a DHCP client. You should keep this configuration in case your service provider supports DHCP, or if you are connecting using a dynamic IP address. The server that assigns the gateway with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' and specifying your own mask instead. You can click the 'Release' button to release the current leased IP address. Once the address has been released, the button text changes to 'Renew'. Use the 'Renew' button to renew the leased IP address.

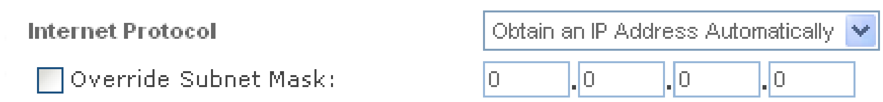


Figure 6.237 Internet Protocol Settings – Automatic IP

Use the Following IP Address Your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.

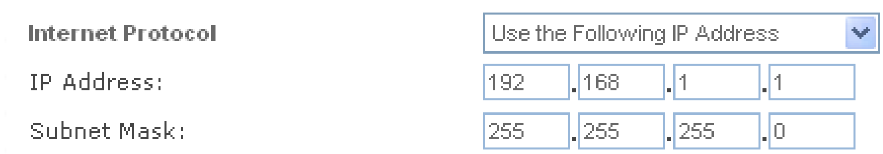


Figure 6.238 Internet Protocol – Static IP

6.4.16.2.3 Advanced

This sub-tab enables you to edit the VLAN's advanced settings.

- **Internet Connection Firewall** Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

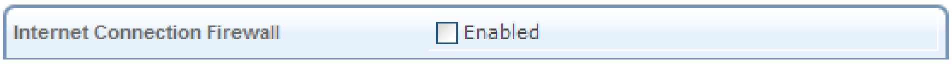


Figure 6.239 Internet Connection Firewall

Internet Connection Fastpath Select this check box to utilize the *Fastpath* algorithm for enhancing packet flow, resulting in faster communication between the LAN and the WAN. By default, this feature is enabled.

Figure 6.240 Internet Connection Fastpath

- **Additional IP Addresses** You can add alias names (additional IP addresses) to the gateway by clicking the 'New IP Address' link. This enables you to access the gateway using these aliases in addition to the 192.168.1.1 and the http://openrg.home.

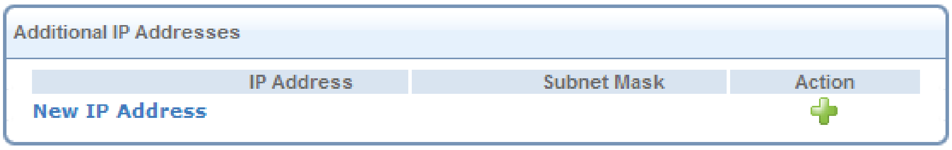


Figure 6.241 Additional IP Addresses

6.4.16.2.4 DSCP Remark According to 802.1p CoS

When creating a VLAN interface over a LAN connection, it is possible to determine the IP header's Differentiated Services Code Point (DSCP) priority value according to the VLAN header's 802.1p Class of Service (CoS) tag. The DSCP value can then be used for Quality of Service (Qos) traffic prioritization. For more information, refer to Section 5.3.

Figure 6.242 DSCP Remark According to 802.1p CoS

1. Select the 'Enabled' check-box. The screen refreshes, displaying the following table.

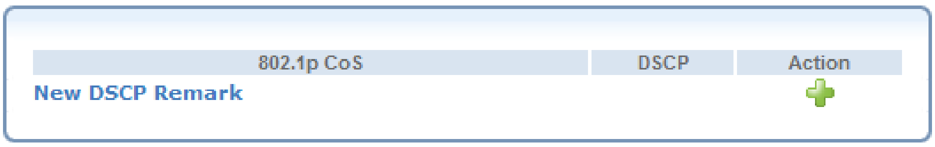


Figure 6.243 DSCP Remarks Table

2. Click the 'New DSCP Remark' link. The following screen appears.

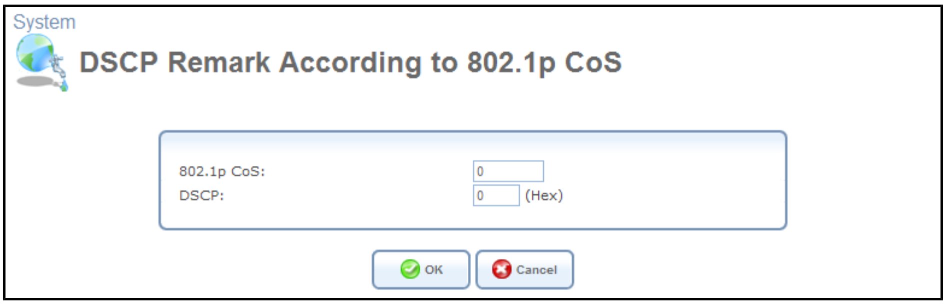


Figure 6.244 DSCP Remark Entry Settings

3. Enter the 802.1p CoS and DSCP values to be associated, and click 'OK'. The new pair of values will appear in the table.

4. Click 'OK' to save the settings.

6.4.16.3 VLAN Use Case

The following example demonstrates the advantages of a VLAN interface through practical setup and performance measurements. The VLAN interface in this example is used to grant prioritization to specific traffic, providing a basic level of Quality of Service (refer to Section 5.3).

6.4.16.3.1 Hardware Requirements

This use case requires the following:

- A development board
- Two equal Linux LAN hosts holding two identical 100MB files
- A 10 Mbps switch (optional)
- A WAN host serving as an FTP server

6.4.16.3.2 Physical Setup

Since this example requires overloading the WAN, the WAN network segment bandwidth must be less than the LAN's. This can be achieved, for example, by either connecting OpenRG's WAN to a 10 Mbps switch, or by forcing the FTP server's WAN interface to 10 Mbps.

1. Connect the two LAN hosts to the development board's LAN ports.

2. Connect the board's WAN port to the 10 Mbps switch, and the switch to the WAN.

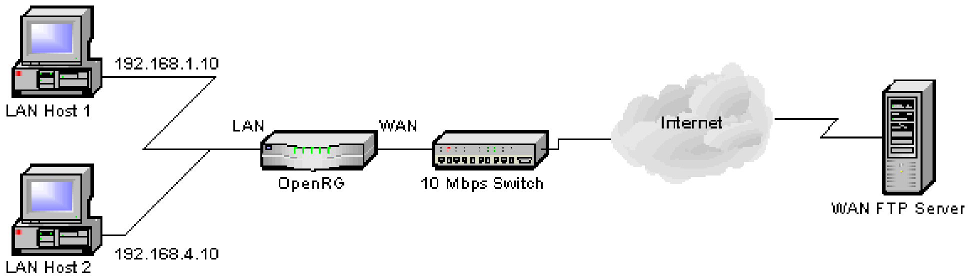


Figure 6.245 Physical Setup

6.4.16.3.3 OpenRG Configuration

To configure the VLAN interface, perform the following steps:

1. In the 'Network Connections' screen, delete the LAN bridge (if one exists) by clicking its action icon . Click 'OK' in the attention screen to confirm the deletion. The LAN Ethernet that was enslaved to the bridge will automatically be configured with the IP address 192.168.1.1, and serve as the DHCP server for this subnet.

2. Create a VLAN interface over the LAN Ethernet, using the Advanced utility of the connection wizard. The underlying device should be LAN Ethernet (or LAN Hardware Ethernet Switch, depending on your platform). Set the VLAN ID to 100.

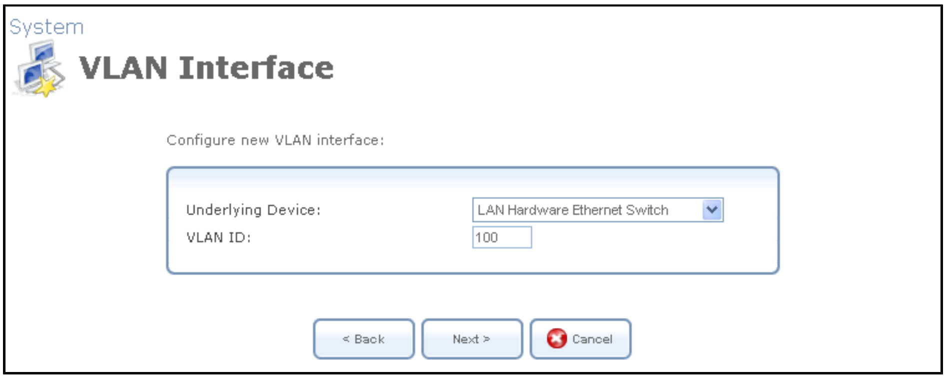


Figure 6.246 VLAN Interface Configuration

3. In the 'Connection Summary' screen, check the 'Edit the Newly Created Connection' check box and click Finish. The 'LAN Ethernet Properties' screen appears:

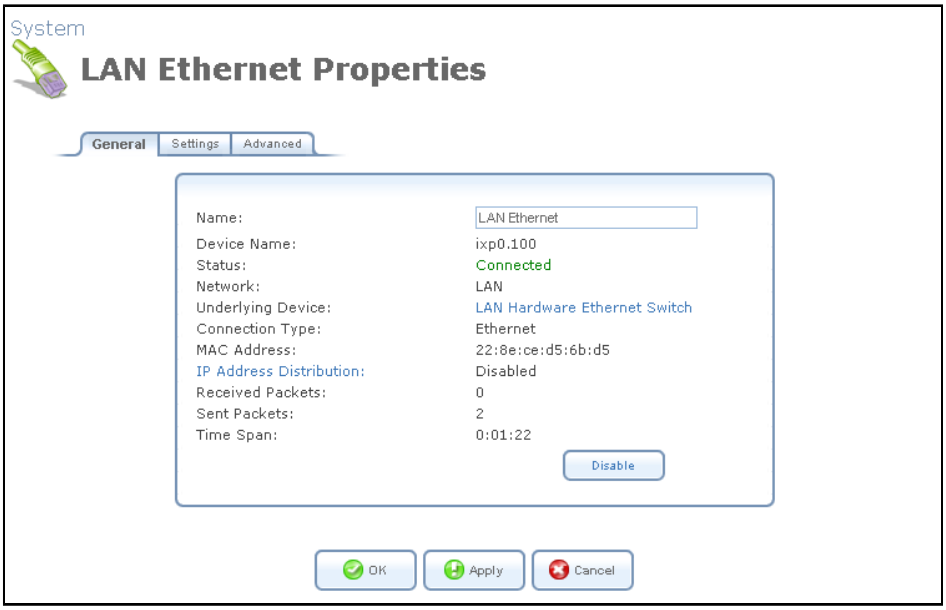


Figure 6.247 LAN Ethernet Properties

4. Click the Settings tab, and in the Internet Protocol section, select "Use the Following IP Address" from the drop-down menu. The screen refreshes (see Figure 6.248).

5. Enter 192.168.4.1 as the IP address and 255.255.255.0 as the subnet mask.

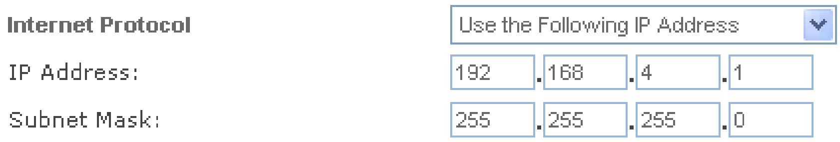


Figure 6.248 Internet Protocol

6. In the IP Address Distribution section, select "DHCP Server" from the drop-down menu. The screen refreshes (see Figure 6.249).

7. Enter 192.168.4.2 as the start IP address and 192.168.4.254 as the end IP address. Enter 255.255.255.0 as the subnet mask. Leave all other fields at their defaults.

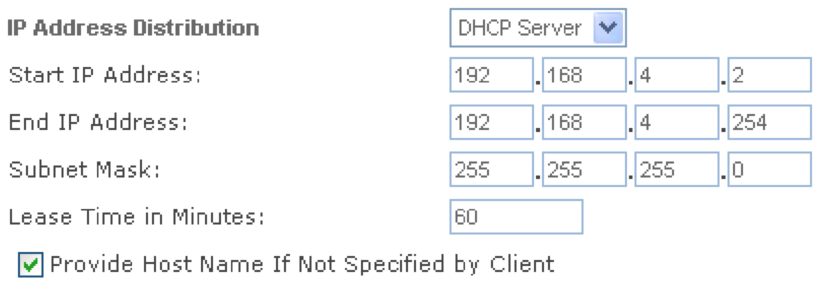


Figure 6.249 IP Address Distribution

8. Click the Advanced tab, and verify that the Internet Connection Firewall is disabled.

Figure 6.250 Internet Connection Firewall

9. Click 'OK' to save the settings.

6.4.16.3.4 Host 1 Configuration

This computer will act as an ordinary LAN host connected to OpenRG with no special settings. After connecting the computer to the gateway, use the following command (in the Linux shell command line) to obtain an IP address from OpenRG:

```
# pump -i eth0
```

Verify that the obtained IP address is in OpenRG's default subnet (192.168.1.x) using this command:

```
# ifconfig eth0
```

6.4.16.3.5 Host 2 Configuration

This computer will act as a VLAN-capable host connected to OpenRG. Use the following command to create the VLAN interface (verify that the `vconfig` utility is installed on this host's Linux operating system):

```
# vconfig add eth0 100
```

After connecting the computer to the gateway, use the following command (in the Linux shell command line) to obtain an IP address from OpenRG:

```
# pump -i eth0.100
```

Verify that the obtained IP address is in OpenRG's VLAN subnet (192.168.4.x) using this command:

```
# ifconfig eth0.100
```

6.4.16.3.6 Running the Scenario

1. Open an FTP connection from both hosts to the WAN FTP server. Use an FTP client that displays throughput rates.

2. Initiate an FTP **upload** of the 100MB files from both hosts to the server simultaneously. Observe that the throughput rates on both hosts are similar - approximately half of the forced WAN bandwidth (5MB each).

3. Configure the VLAN interface of Host 2 to add priority to VLAN frames, using the following command:

   ```
   # vconfig set_egress_map eth0.100 0 7
   ```

4. Repeat the FTP upload test and observe that the throughput rate of Host 2 increases significantly at the expense of Host 1.

6.4.16.4 VLAN Bridge Use Case

OpenRG enables you to partition an Ethernet-based network by creating segregated virtual networks. Such network topology can be effectively used, for example, in the following real-life situation.

A company's workstations are connected to the same physical network, and all of them receive an IP from the same DHCP server. However, all of the R&D department workstations need to be connected to a separate file server, to which the rest of the company's workstations do not have access. At the same time, the R&D workstations should not have access to the file server that belongs, for example, to the Marketing department.

To create such a network topology, you can set up a *VLAN bridge* and connect all the workstations to it in the manner depicted in the following figure.

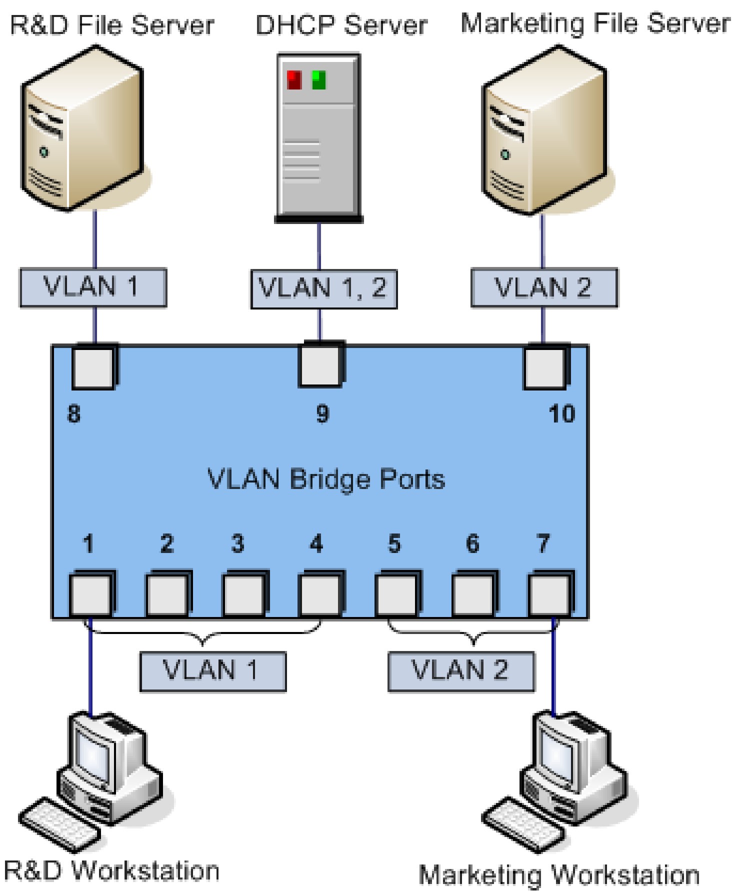


Figure 6.251 VLAN Bridge

The DHCP server is configured to handle both VLANs, and can distinct between requests sent from the R&D workstations and requests from the Marketing workstations.

The advantage of this method of network management is that any workstation can be moved from network to network without a need for any physical (wiring) modification. The only thing

a system administator has to do is to reconfigure the VLAN bridge by changing the default VLAN ID for a certain port.

Note: The following procedure is appropriate only for platforms with LAN hardware switch ports that support PVID.

To set up a VLAN bridge on OpenRG, perform the following:

1. In the 'Network Connections' screen under 'System' (see Figure 6.13), click the 'New Connection' link. The 'Connection Wizard' screen appears (see Figure 6.14).
2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears.

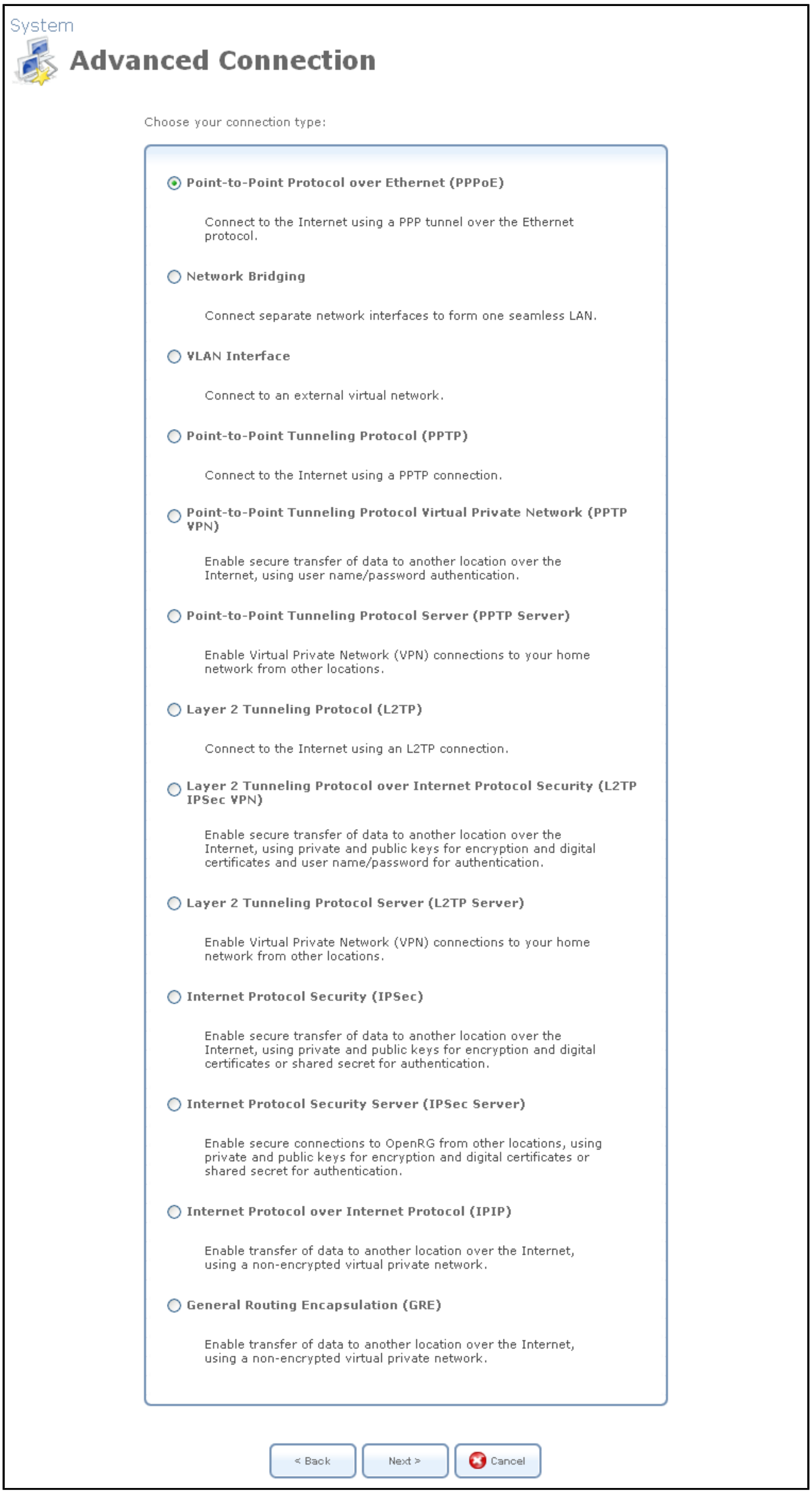


Figure 6.252 Advanced Connection Wizard

3. Select 'Network Bridging' and click 'Next'. The 'Bridge Options' screen appears.

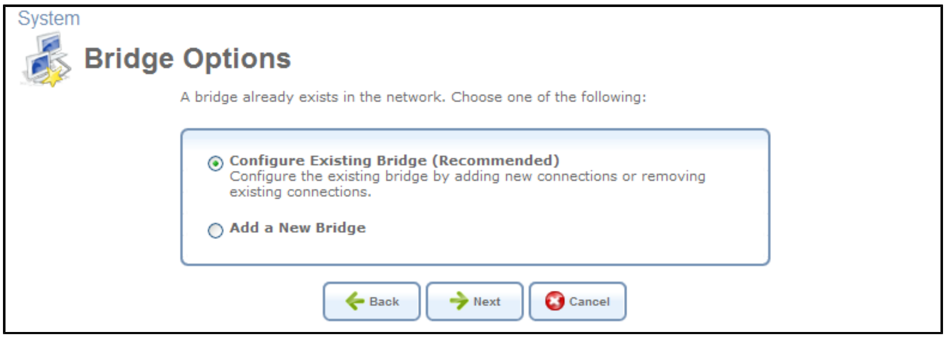


Figure 6.253 Bridge Options

4. Select the 'Configure Existing Bridge' option and click 'Next'. The 'Network Bridging' screen appears.

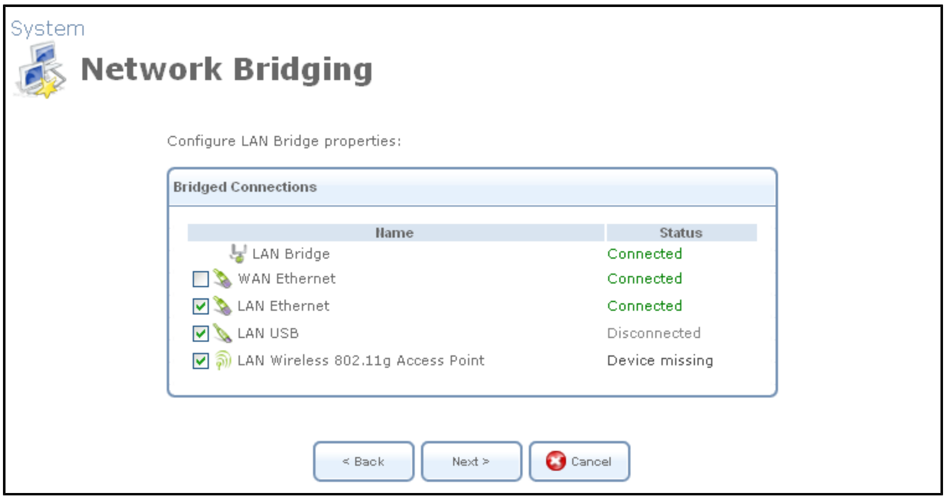


Figure 6.254 Network Bridging – Configure Existing Bridge

5. Select the 'WAN Ethernet' check box and click 'Next'. A LAN-WAN bridge is created, and the 'Connection Summary' screen appears, corresponding to your changes.

Figure 6.255 Connection Summary – Configure Existing Bridge

6. Click 'Finish' to save the settings.

7. Back in the 'Network Connections' screen, click the 'LAN Bridge' link, and select 'Bridging. The following screen appears.

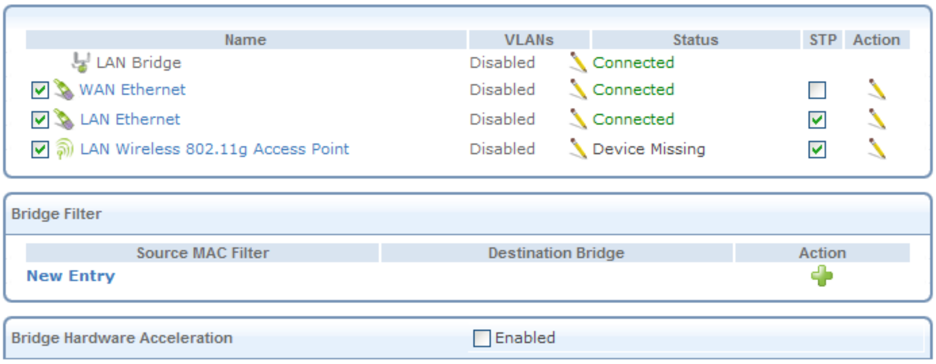


Figure 6.256 LAN Bridge Properties – Bridging

8. Under the 'VLANs' column, click the action icon of the WAN Ethernet connection. The connection's 'VLAN Settings' screen appears.

Figure 6.257 VLAN Settings

9. Select the 'Enable VLAN' check box, and click 'Apply'. The screen refreshes, adding the 'VLAN IDs' section.

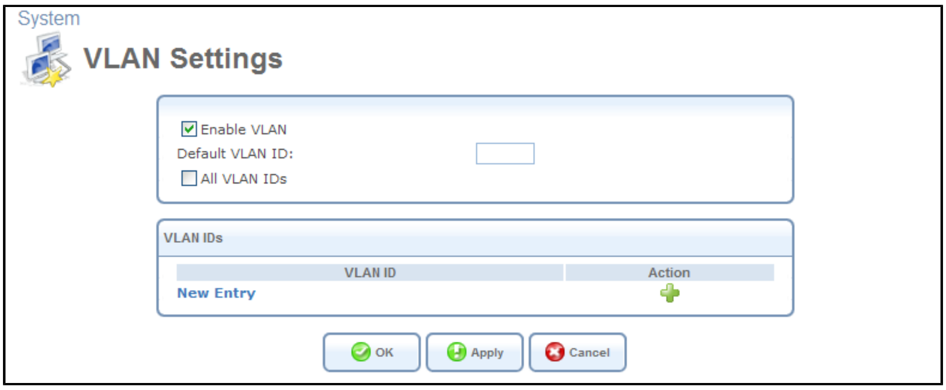


Figure 6.258 VLAN Settings – Add VLAN ID

10. Define **VLAN 1** and then **VLAN 2** by going through the following steps:

   a. Click the 'New Entry' link. The 'VLAN ID Settings' screen appears.

Figure 6.259 VLAN ID Settings

b. In the 'VLAN ID' field, enter a number that will serve as a VLAN ID (in this example, 1 and 2).

c. Click 'OK' to save settings. The defined VLAN entries appear in the 'VLAN Settings' screen.

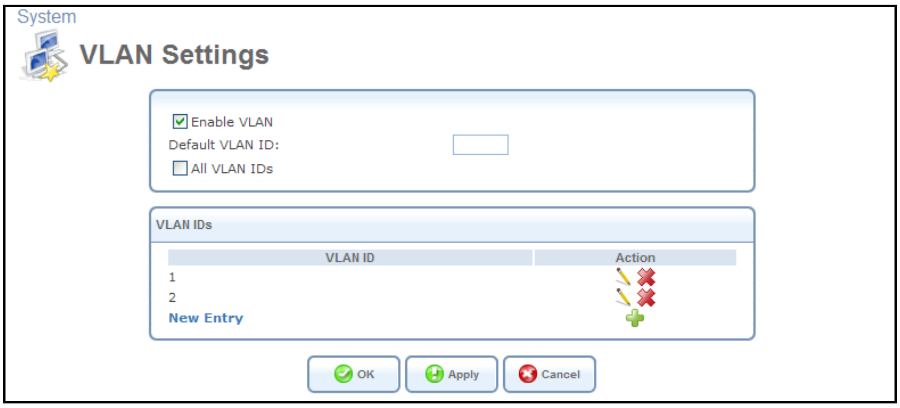


Figure 6.260 VLAN Settings – Added VLANs

d. Click 'OK'. You are redirected back to the 'Bridging' section of the 'LAN Bridge Properties' screen (see Figure 6.256).

11. Under the 'VLANs' column, click the action icon of the LAN Hardware Ethernet Switch connection. The connection's 'VLAN Settings' screen appears (see Figure 6.257).

12. Define the two VLAN IDs on the LAN Hardware Ethernet Switch connection exactly as on the WAN Ethernet one.

13. Configure each of the involved switch ports with a specific VLAN ID:

a. In the 'Network Connections' screen, click the 'LAN Hardware Ethernet Switch' link, and select 'Switch'. The following screen appears.

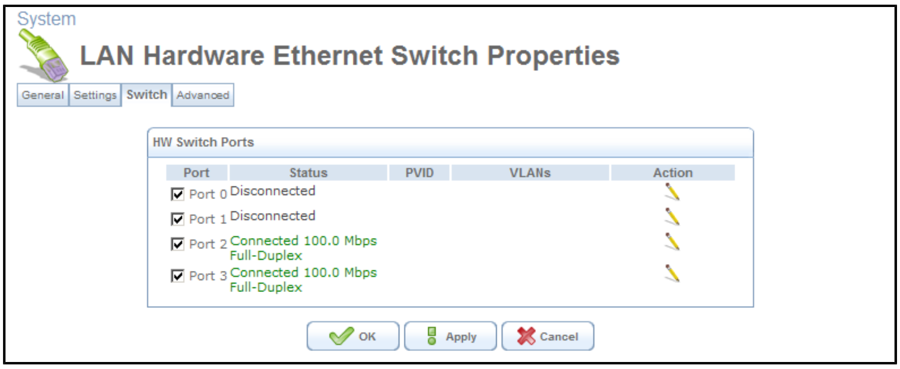


Figure 6.261 LAN Hardware Ethernet Switch Properties – Switch

b. Click the action icon that corresponds to the port you would like to configure. The 'Port Settings' screen appears.

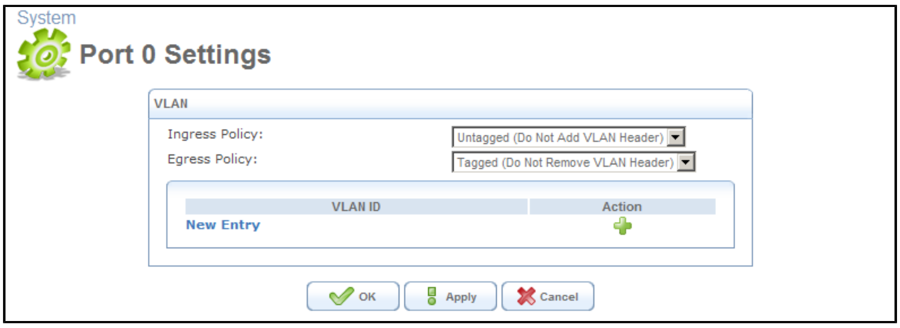


Figure 6.262 Port Settings

c. From the 'Ingress Policy' drop-down menu, select the 'Tagged' option. The screen refreshes, displaying the 'Default VLAN ID' field (see Figure 6.263).

d. Enter an ID of the VLAN that will be created on the port. The incoming (ingress) frames will be marked with this ID.

e. From the 'Egress Policy' drop-down menu, select the 'Untagged' option.

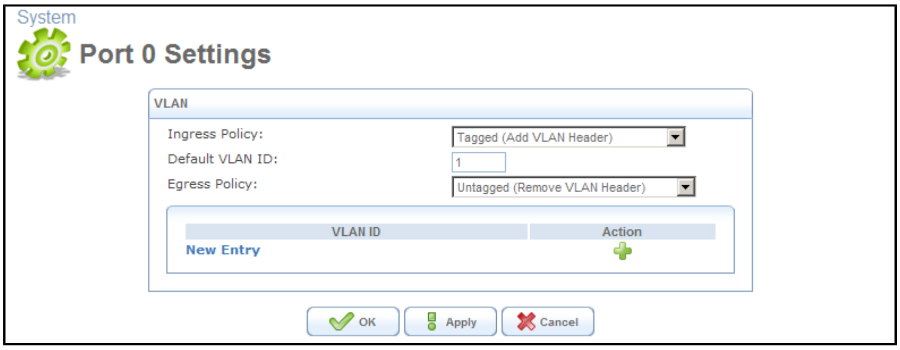


Figure 6.263 Port Settings – VLAN

f. Click 'OK' to save the settings. OpenRG will request browser reloading.

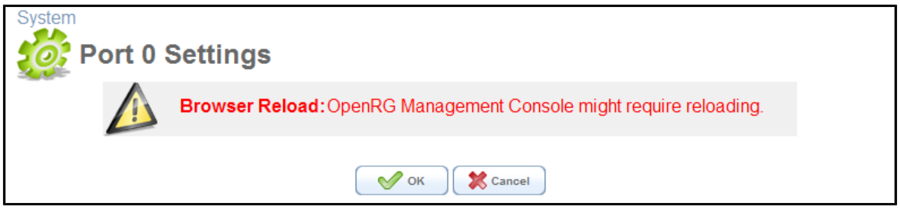


Figure 6.264 Port Settings – Browser Reloading

g. Click 'OK' to proceed. After the 'Port Settings' screen is back, the default VLAN ID appears in the dedicated VLAN ID entries table.

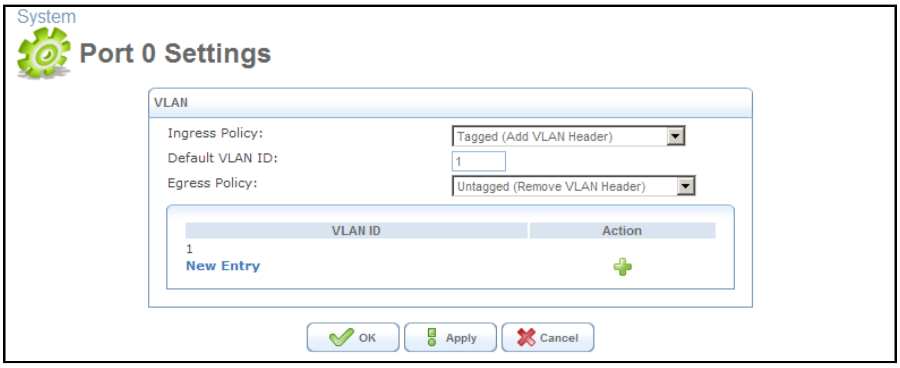


Figure 6.265 Port Settings – Default VLAN ID

h. Click 'OK'. You are redirected back to the 'LAN Hardware Ethernet Switch Properties' screen, in which the configured port's VLAN ID is displayed.

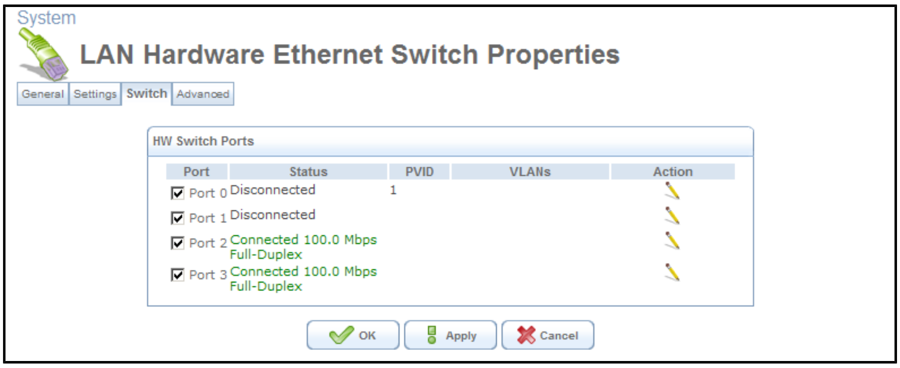


Figure 6.266 Port Settings – Default VLAN ID

i. Perform the same procedure on each of the ports you will be using.

14. Verify that IP forwarding is disabled on your DHCP server.

To verify that there is no communication between the two VLANs, perform the following test:

1. Connect two hosts to the ports that belong to different VLANs. Each of the hosts will be assigned an IP with a different subnet by the DHCP server.

2. Ping each host from another one. If you have successfully performed the aforementioned procedure, the ping test will fail. This means that the traffic of each VLAN is segregated.

6.4.16.5 Port-based VLAN Tagging

A LAN device can obtain a VLAN tag (identifier) from its LAN switch port settings. This section describes several configuration options in order to achieve port-based VLAN tagging on OpenRG.

This example may suit a scenario where three hosts and a SIP telephone are connected to the gateway. Each of these LAN devices must be assigned with a different VLAN ID and priority when it communicates through the WAN. The following are the assumptions regarding the current network topology and setup:

- A LAN bridge connects the Ethernet switch and WLAN interfaces.
- The WAN connection is DHCP/Ethernet.
- Two VLAN IDs will be used: one for traffic received on port 3 on the LAN Ethernet switch (connected to the IP phone), and the other for all other traffic, generated by the hosts connected to the other Ethernet switch ports and through the WLAN interface. This example can be extended to support more VLAN subnets.

6.4.16.5.1 Option A: Bridge Mode

In this option VLAN interfaces are not configured. All LAN traffic is bridged to the WAN, with different VLAN IDs depending on the receiving LAN Ethernet switch port. You must simply adjust the LAN Ethernet switch port settings for each port, so that it tags received packets with a VLAN ID. You must connect the WAN Ethernet device to the bridge, and configure the bridge to receive and transmit tagged traffic on the Ethernet WAN device.

Based on the Rx port, you can add VLAN IDs on outgoing packets. To mark the packets received on each of the LAN switch ports with different VLAN ID, perform the following:

1. In the WBM, click the 'Device' menu item under the 'Local Network' tab. The 'Device' screen appears.

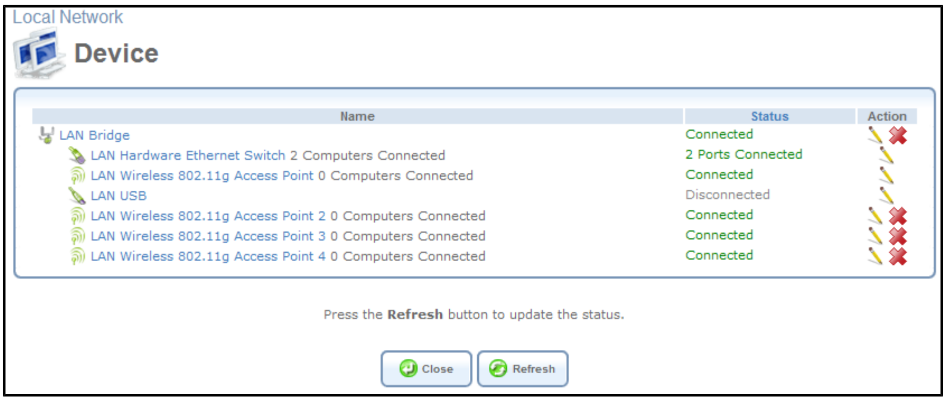


Figure 6.267 Local Network Device View

2. Click the 'LAN Hardware Ethernet Switch' link (or its action icon).

3. In the 'LAN Hardware Ethernet Switch Properties' screen, click the 'Switch' sub-tab.

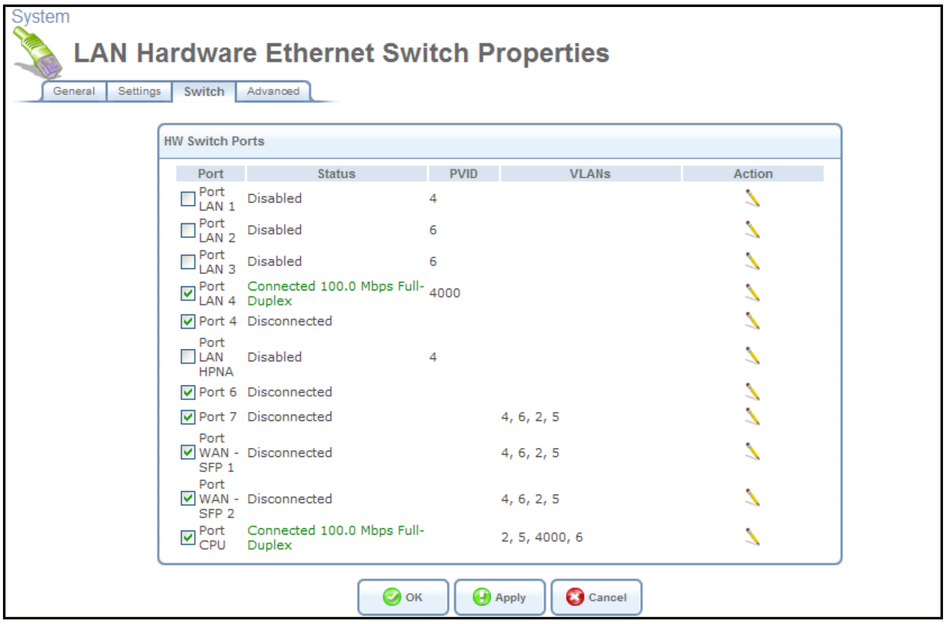


Figure 6.268 Switch

4. Click a port's  action icon . The 'Port LAN Settings' screen appears.

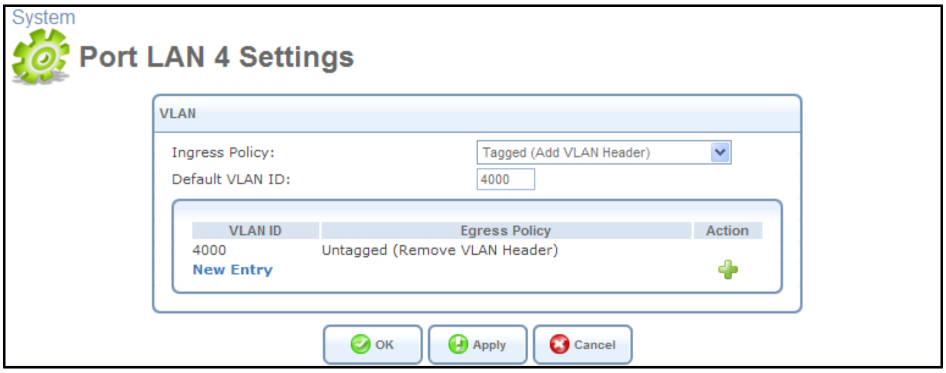


Figure 6.269 Port LAN Settings

5. In the 'Ingress Policy' drop-down menu, select 'Tagged (Add VLAN Header)'.

6. Under the 'VLAN ID' column, click 'New Entry' in order to add identifiers to the VLAN.

6.4.16.5.2 Option B: Mixed Bridge/Route Mode

In this option, you will configure two VLAN interfaces over the WAN Ethernet device, and one VLAN interface over the LAN bridge. The LAN VLAN interface is used to distinguish the traffic on switch port 3 from the traffic on other switch ports and WLAN interface. Traffic is bridged from the LAN VLAN interface to the first WAN VLAN interface. All other traffic is routed to the second WAN VLAN interface. To set the 802.1p value of the packets according to the receiving interface, you must configure a QoS packet priority output rule on each WAN VLAN interface.

Configure the LAN VLAN interface:

1. In the WBM, click the 'Network Connections' menu item under the 'System' tab, and then click the 'New Connection' link. The Connection Wizard commences.

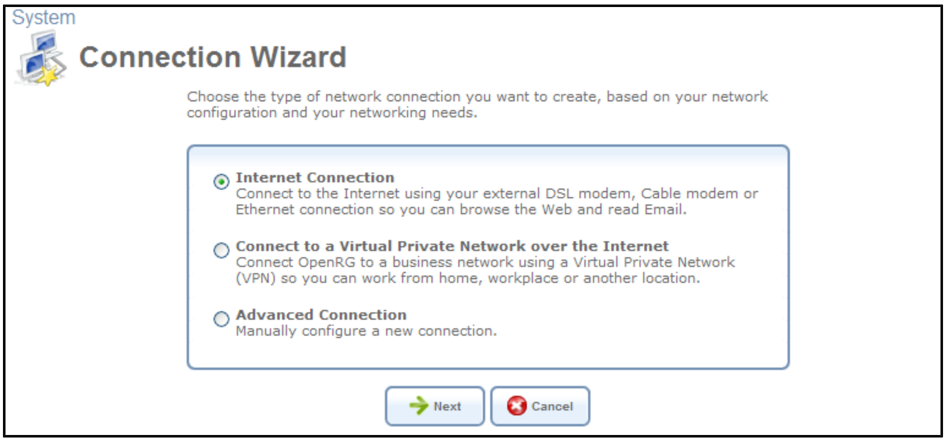


Figure 6.270 Connection Wizard

2. Select 'Advanced Connection' and click 'Next'.

3. Select 'VLAN Interface' and click 'Next'.

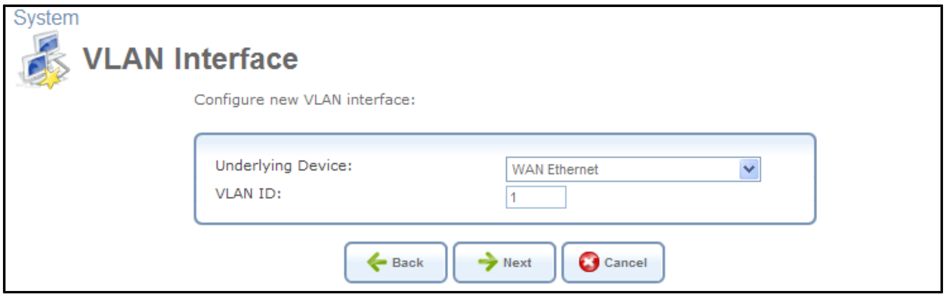


Figure 6.271 VLAN Interface

4. Select 'LAN Bridge' as the underlying device, and provide a VLAN ID. Click 'Next'.

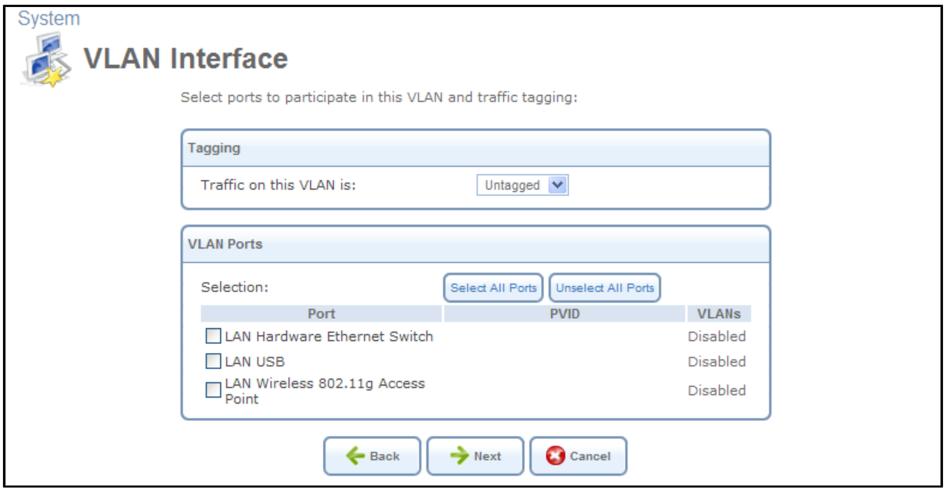


Figure 6.272 VLAN over LAN Bridge

5. In the 'Tagging' section, select 'Tagged'. In the 'VLAN Ports' section, check 'LAN Hardware Ethernet Switch' and port 3. Click 'Next' and then 'Finish'.

The newly created LAN VLAN interface has no IP address. Its traffic will be bridged to the WAN VLAN. The IP devices connected to the LAN Ethernet switch port 3 are assumed to have a public IP address.

Configure the WAN VLAN interface:

1. Follow the instructions above, but in the 'VLAN Interface' screen, select 'WAN Ethernet' as the underlying device and provide a VLAN ID. Click 'Next'. The 'Connection Summary' screen appears.

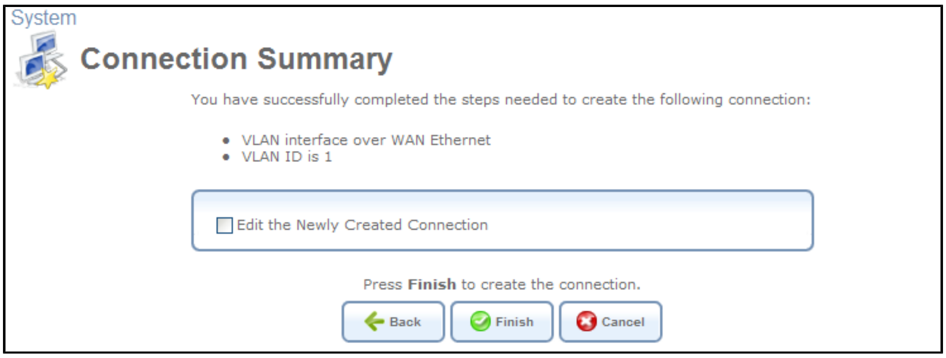


Figure 6.273 Connection Summary

2. Select the 'Edit the Newly Created Connection' check box and click 'Finish'.

3. In the 'WAN Ethernet VLAN Properties' screen, click the 'Routing' sub-tab and deselect the 'Default Route' field.

6.4.16.5.3 Option C: DSCP-based Routing

In this option, traffic from LAN is routed (and NATed) to the WAN rather than bridged. You must configure two VLAN interfaces over the WAN Ethernet device, and one VLAN interface over the LAN bridge. You will use the QoS rules to set the DSCP value on the packets arriving on the LAN VLAN interface. The routing decision will be based on the DSCP value, using DSCP-based static route rules. Traffic from the LAN VLAN will be routed to the first WAN VLAN, and use the second WAN VLAN as default route. DSCP values are translated into 802.1p priority by the QoS module.

6.4.17 Setting Up an IPIP Tunnel

OpenRG allows you to create an Internet Protocol over Internet Protocol (IPIP) tunnel to another router, by encapsulating IP packets in IP. This tunnel can be managed as any other network connection. Supported by many routers, this protocol enables using multiple network schemes. Note, however, that IPIP tunnels are not secured.

6.4.17.1 Creating an IPIP Tunnel

To create a new IPIP tunnel, perform the following:

1. In the 'Network Connections' screen under 'System' (see Figure 6.13), click the 'New Connection' link. The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears.

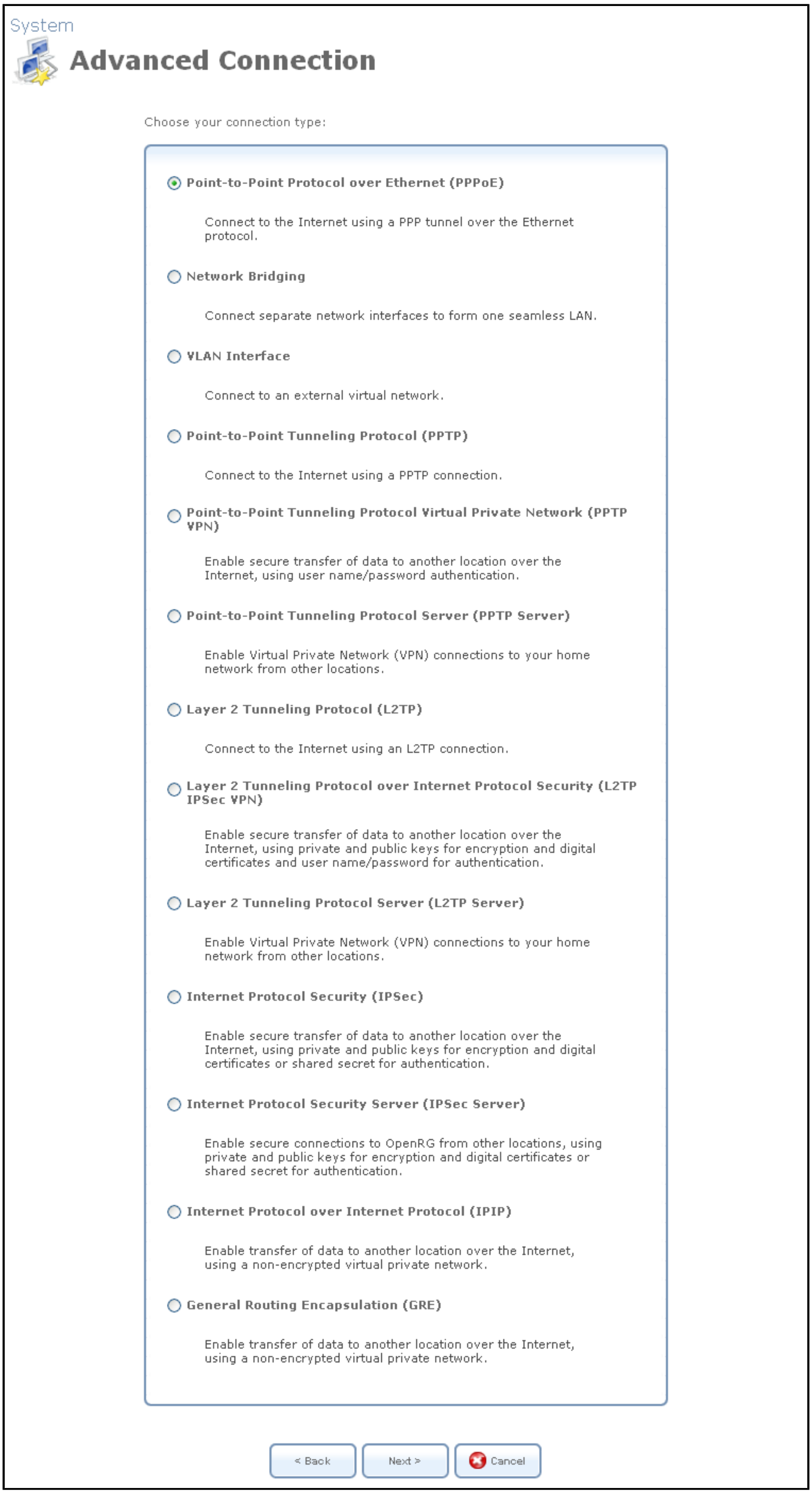


Figure 6.274 Advanced Connection Wizard

3. Select the 'Internet Protocol over Internet Protocol (IPIP)' radio button and click 'Next'. The 'Internet Protocol over Internet Protocol (IPIP)' screen appears.

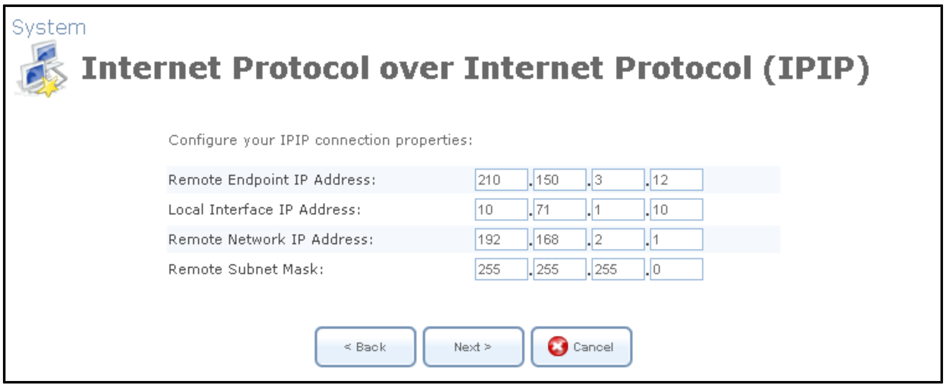


Figure 6.275 Internet Protocol over Internet Protocol (IPIP)

4. Enter the tunnel's remote endpoint IP address.

5. Enter the local IP address for the interface.

6. Enter the IP address and subnet mask of the remote network that will be accessed via the tunnel, and click 'Next'. The 'Connection Summary' screen appears.

Figure 6.276 Connection Summary

7. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

8. Click 'Finish' to save the settings.

The new IPIP tunnel will be added to the network connections list, and will be configurable like any other connection.

6.4.17.2 Viewing and Editing the Tunnel Settings

To view and edit the IPIP tunnel settings, click the 'WAN IPIP' link in the 'Network Connections' screen (see Figure 6.13). The 'WAN IPIP Properties' screen appears.

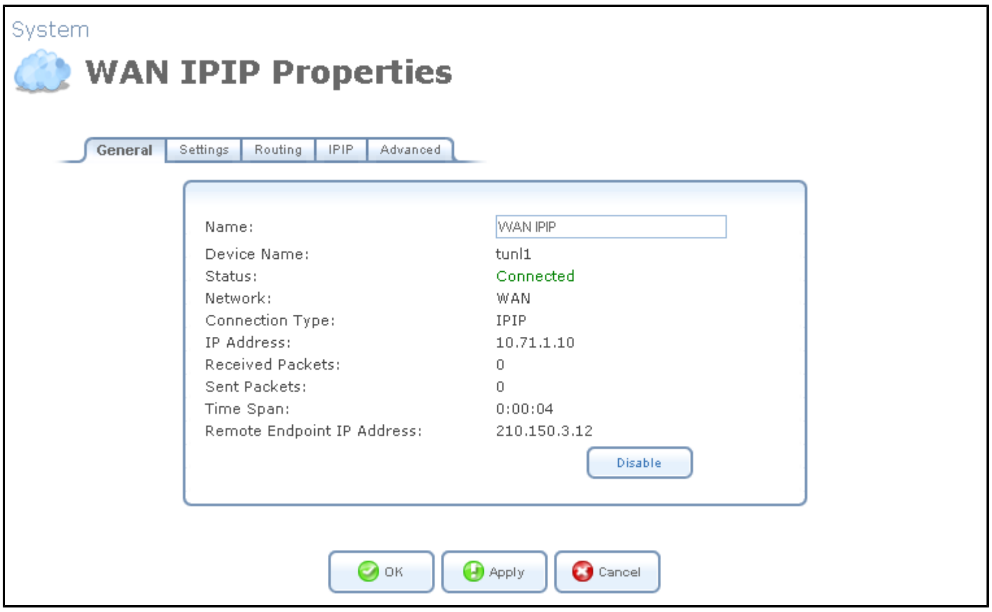


Figure 6.277 WAN IPIP Properties

6.4.17.2.1 General

This sub-tab enables you to view a detailed summary of the IPIP tunnel settings (see Figure 6.277). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.17.2.2 Settings

This sub-tab enables you to edit the following IPIP tunnel settings.

General This section displays the tunnel's general parameters.

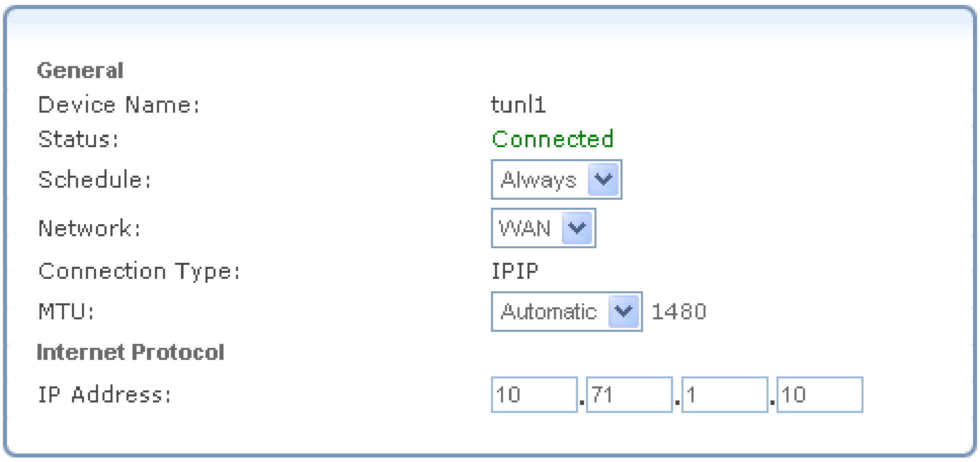


Figure 6.278 General WAN IPIP Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol The local IP address for the interface.

6.4.17.2.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

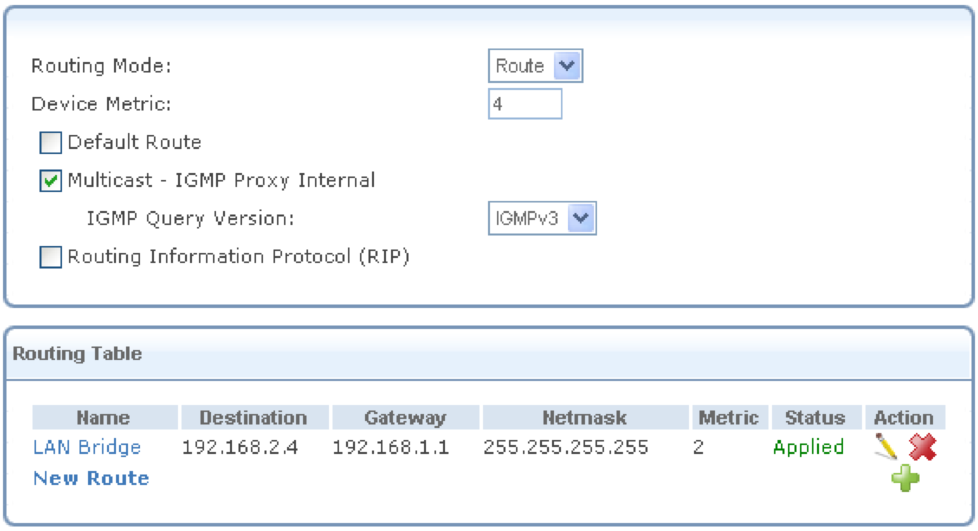


Figure 6.279 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
- **Send RIP messages**—select either 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.

Routing Table Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.
To learn more about this feature, refer to Section 6.6.

6.4.17.2.4 IPIP

This sub-tab enables you to edit the tunnel's remote endpoint IP address.

Figure 6.280 IPIP

6.4.17.2.5 Advanced

This sub-tab enables you to edit the tunnel's advanced settings.

- **Internet Connection Firewall** Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the

Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

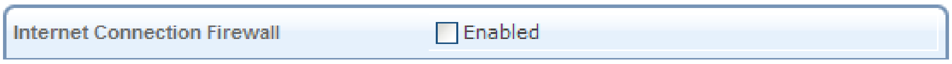


Figure 6.281 Internet Connection Firewall

6.4.18 Setting Up a GRE Tunnel

OpenRG allows you to create a General Routing Encapsulation (GRE) tunnel in order to transport multicast traffic and IPv6, in addition to other existing tunneling capabilities (for example, IPIP, L2TP, PPTP).

6.4.18.1 Creating a GRE Tunnel

To create a new GRE tunnel, perform the following:

1. In the 'Network Connections' screen under 'System' (see Figure 6.13), click the 'New Connection' link. The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears.

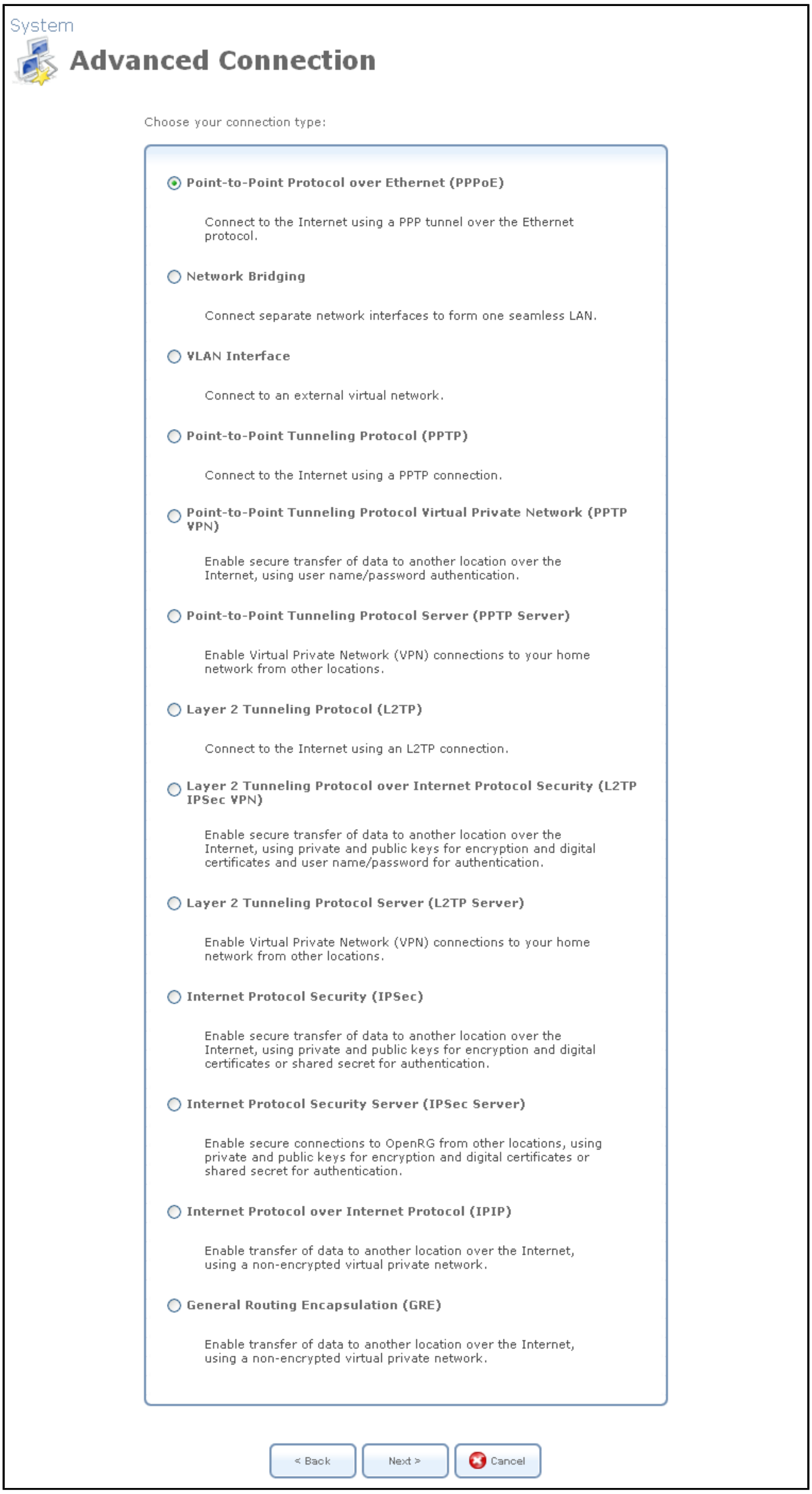


Figure 6.282 Advanced Connection Wizard

3. Select the 'General Routing Encapsulation (GRE)' radio button and click 'Next'. The 'General Routing Encapsulation (GRE)' screen appears.

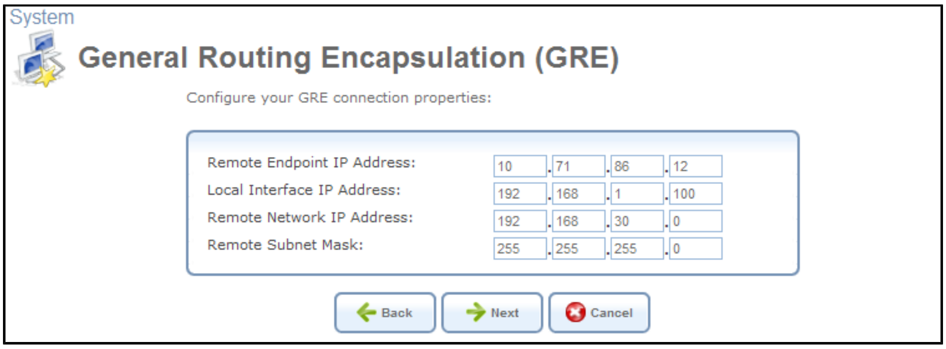


Figure 6.283 General Routing Encapsulation (GRE)

4. Enter the tunnel's remote endpoint IP address.

5. Enter the local IP address of the gateway's GRE interface.

6. Enter the IP address and subnet mask of the remote network that will be accessed via the tunnel, and click 'Next'. The 'Connection Summary' screen appears.

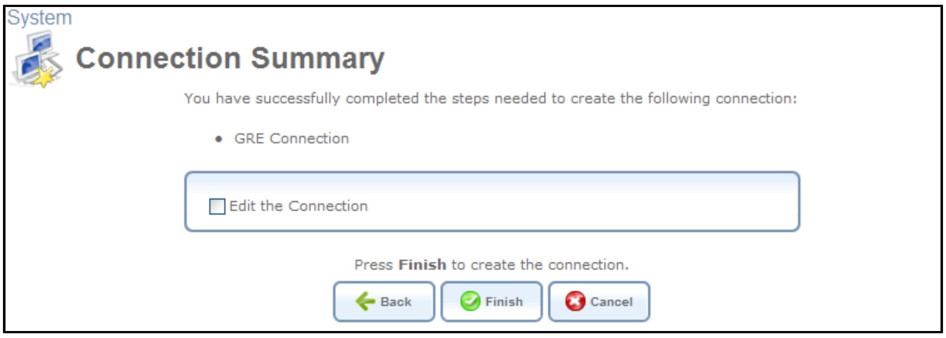


Figure 6.284 Connection Summary

7. Select the 'Edit the Newly Created Connection' check box if you wish to be routed to the new connection's configuration screen after clicking 'Finish'. This screen is described later in this chapter.

8. Click 'Finish' to save the settings.

The new GRE tunnel will be added to the network connections list, and will be configurable like any other connection.

6.4.18.2 Viewing and Editing the Tunnel Settings

To view and edit the GRE connection settings, click the 'WAN GRE' link in the 'Network Connections' screen (see Figure 6.13). The 'WAN GRE Properties' screen appears.

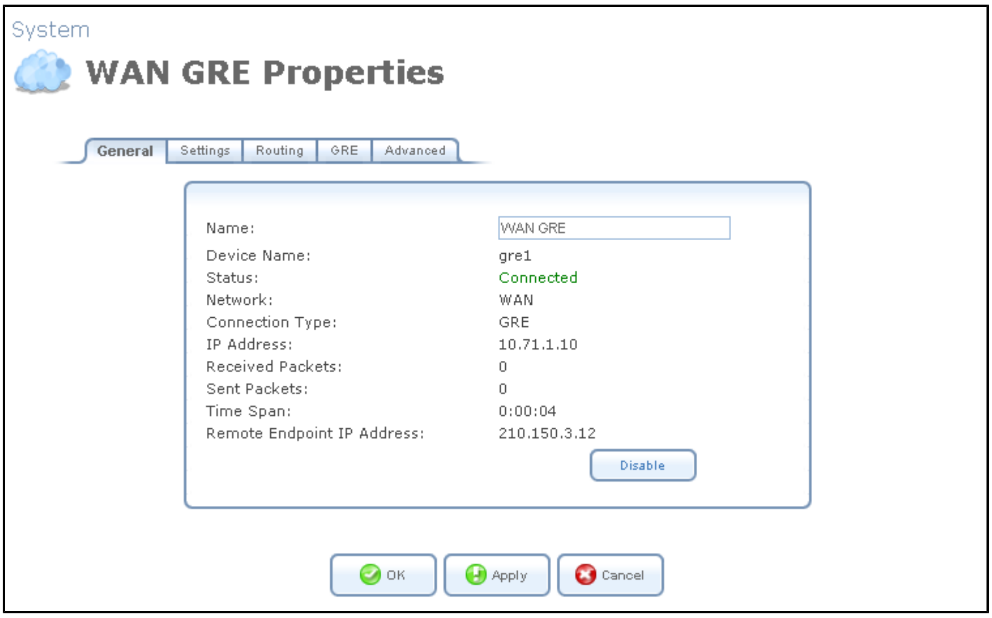


Figure 6.285 WAN GRE Properties

6.4.18.2.1 General

This sub-tab enables you to view a detailed summary of the GRE tunnel settings (see Figure 6.285). These settings can be edited in the rest of the screen's sub-tabs, as described in the following sections.

6.4.18.2.2 Settings

This sub-tab enables you to edit the following GRE tunnel settings.

General This section displays the connection's general parameters.

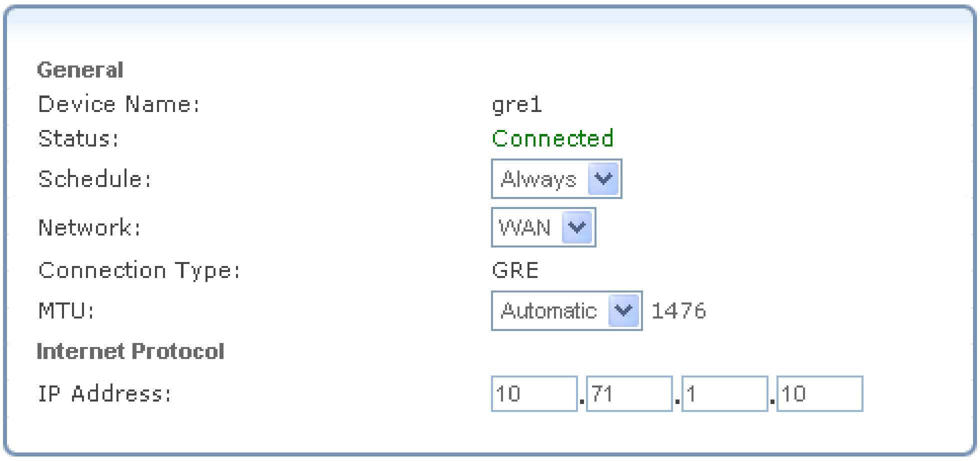


Figure 6.286 General WAN GRE Settings

Schedule By default, the connection will always be active. However, you can configure scheduler rules in order to define time segments during which the connection may be active. Once a scheduler rule(s) is defined, the drop-down menu will allow you to choose between the available rules. To learn how to configure scheduler rules, refer to Section 6.9.3.

Network Select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection, by selecting the connection type from the drop-down menu. For more information, refer to Section 6.4.1. Note that when defining a network connection as DMZ, you must also:

- Remove the connection from under a bridge, if that is the case.
- Change the connection's routing mode to "Route", in the 'Routing' sub-tab.
- Add a routing rule on your external gateway (which may be supplied your ISP), informing of the DMZ network behind OpenRG.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. In the default setting, Automatic, the gateway selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. In case you select 'Manual' it is recommended to enter a value in the 1200 to 1500 range.

Internet Protocol The local IP address for the interface.

6.4.18.2.3 Routing

This sub-tab enables you to configure the connection's routing settings. You can choose to setup your gateway to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

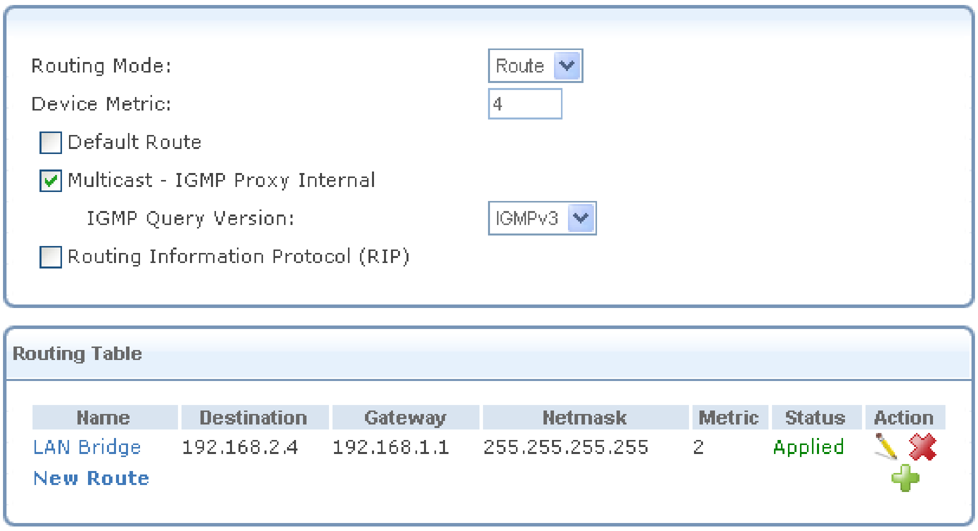


Figure 6.287 Advanced Routing Properties

You can configure the following settings:

Routing Mode Select one of the following routing modes:

Route Use route mode if you want your gateway to function as a router between two networks.

NAPT Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple machines to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the gateway to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Select this check box to define this device as a the default route.

Multicast – IGMP Proxy Internal / Default OpenRG serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) will be able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts will not be able to join multicast groups of WAN multicast servers. When creating a WAN-LAN bridge, this check box must also be deselected.

IGMP Query Version OpenRG supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down menu appears for LAN connections only.

Routing Information Protocol (RIP) Select this check box to enable the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, you can configure the following:

- **Listen to RIP messages**—select either 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
- **Send RIP messages**—select either 'None', 'RIPv1', 'RIPv2-broadcast' or 'RIPv2-multicast'.

Routing Table Allows you to add or modify routes when this device is active. Use the 'New Route' button to add a route or edit existing routes.
To learn more about this feature, refer to Section 6.6.

6.4.18.2.4 GRE

This sub-tab enables you to edit the tunnel's remote endpoint IP address.

Figure 6.288 GRE

6.4.18.2.5 Advanced

This sub-tab enables you to edit the tunnel's advanced settings.

- **Internet Connection Firewall** Your gateway's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the

Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box. To learn more about your gateway's security features, refer to Section 5.2.

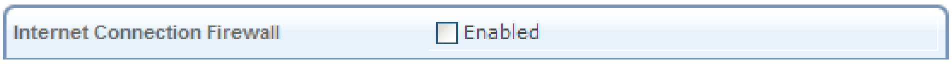


Figure 6.289 Internet Connection Firewall

6.4.18.3 GRE Use Case

The following example demonstrates usage of a GRE interface, to communicate between two hosts that are each in a different LAN, behind separate gateways.

> A GRE tunnel is an unsecured (unencrypted) tunnel. Safety measures must be taken when setting up such a tunnel.

6.4.18.3.1 Hardware Requirements

This use case requires the following:

- Two development boards
- Two LAN hosts
- A WAN host serving as an DHCP server

6.4.18.3.2 Physical Setup

1. Connect each LAN host to a LAN port on a different development board.
2. Connect both boards' WAN ports to the WAN, where a DHCP server is available.

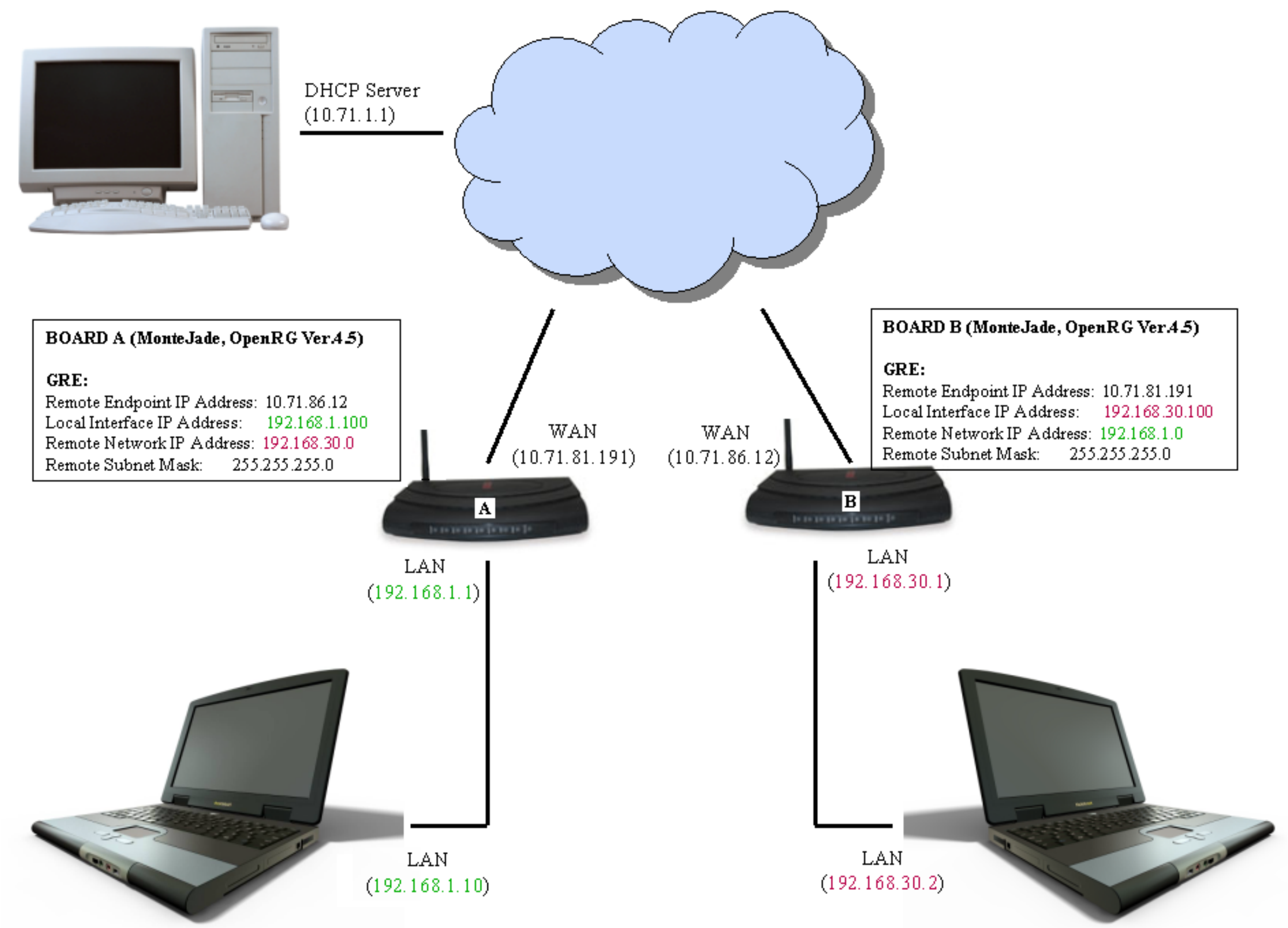


Figure 6.290 Physical Setup

6.4.18.3.3 OpenRG A Configuration

In this example, board A's WAN IP address is 10.71.81.191. In order to create a tunnel, each board must be made aware of the other's WAN IP address (the information must be exchanged).

Create a new GRE tunnel, by performing the following:

1. In the 'Network Connections' screen under 'System' (see Figure 6.13), click the 'New Connection' link. The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears.

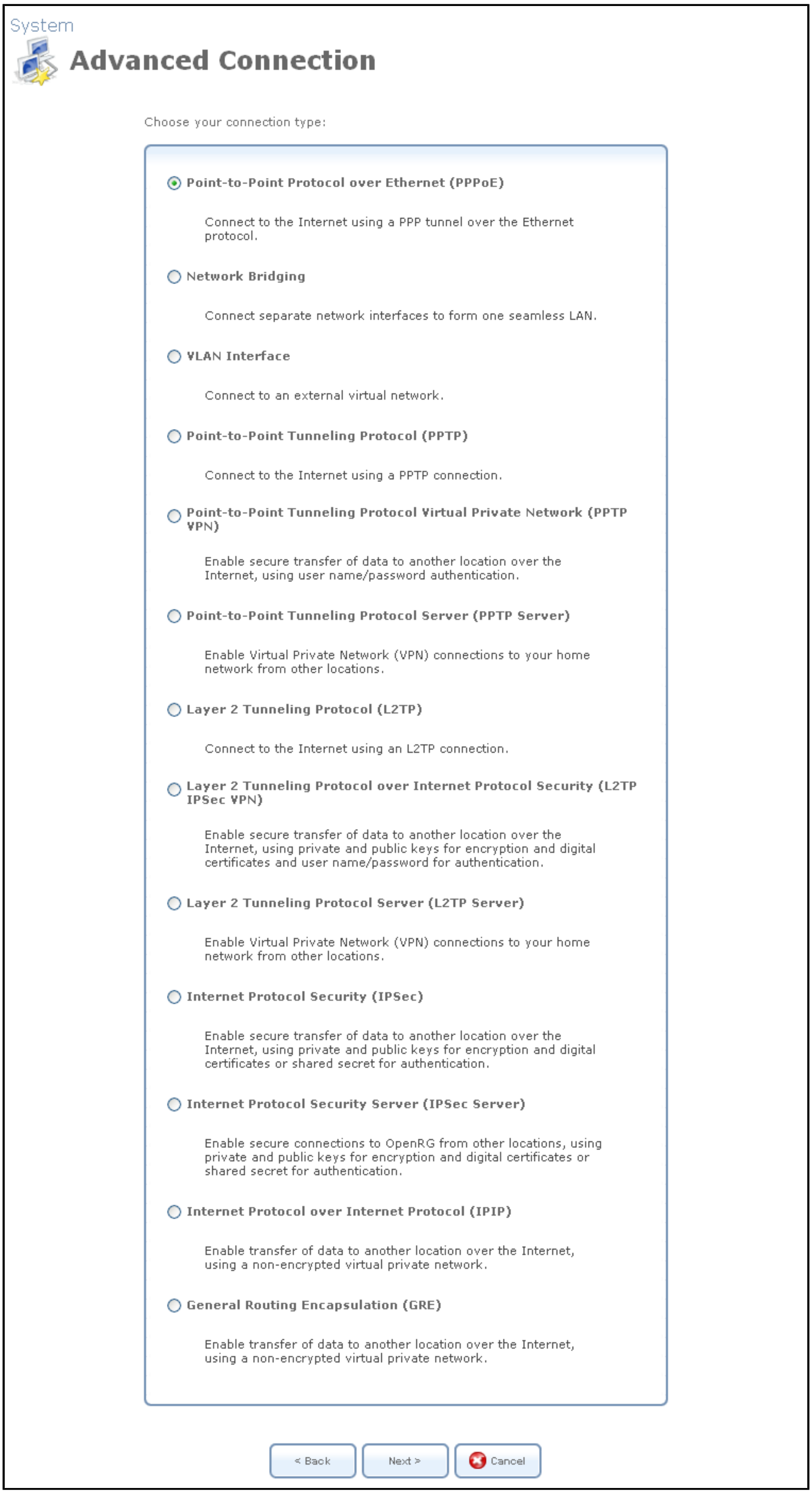


Figure 6.291 Advanced Connection Wizard

3. Select the 'General Routing Encapsulation (GRE)' radio button and click 'Next'. The 'General Routing Encapsulation (GRE)' screen appears.

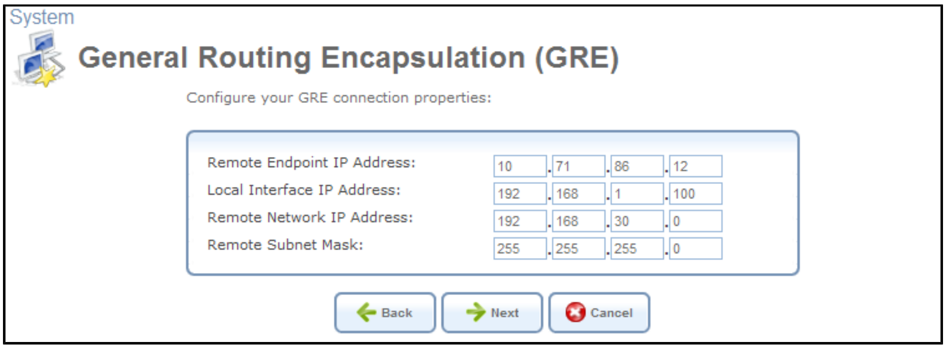


Figure 6.292 General Routing Encapsulation (GRE)

4. Enter 10.71.86.12 as the tunnel's remote endpoint IP address.

5. Enter 192.168.1.100 as the local IP address of this gateway's GRE interface.

6. Enter 192.168.30.0 as the IP address of the remote network that will be accessed via the tunnel, and 255.255.255.0 as the subnet mask. Click 'Next'.

7. In the 'Connection Summary' screen, select the 'Edit the Connection' check box, and click 'Finish'. The 'WAN GRE Properties' screen appears (see Figure 6.285).

8. Click the 'Advanced' sub-tab, and deselect the 'Internet Connection Firewall' check box.

9. Click 'OK' to save the settings.

6.4.18.3.4 OpenRG B Configuration

In this example, board B's WAN IP address is 10.71.86.12. In addition, this board's LAN IP address must be different from that of board A (which has the default 192.168.1.1). In this case it is 192.168.30.1.

Create a new GRE tunnel, by performing the following:

1. In the 'Network Connections' screen under 'System' (see Figure 6.13), click the 'New Connection' link. The 'Connection Wizard' screen appears (see Figure 6.14).

2. Select the 'Advanced Connection' radio button and click 'Next'. The 'Advanced Connection' screen appears.

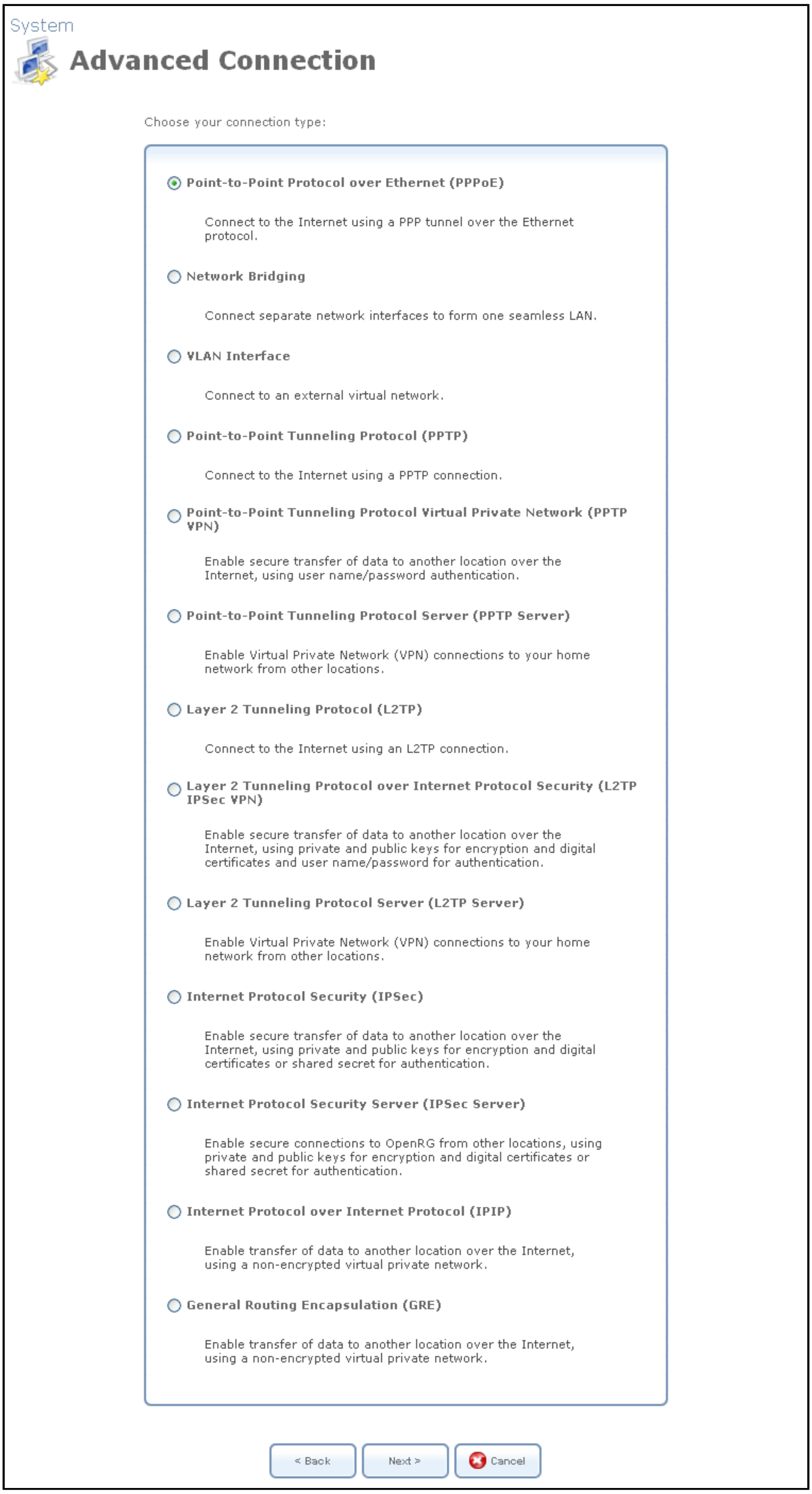


Figure 6.293 Advanced Connection Wizard

3. Select the 'General Routing Encapsulation (GRE)' radio button and click 'Next'. The 'General Routing Encapsulation (GRE)' screen appears.

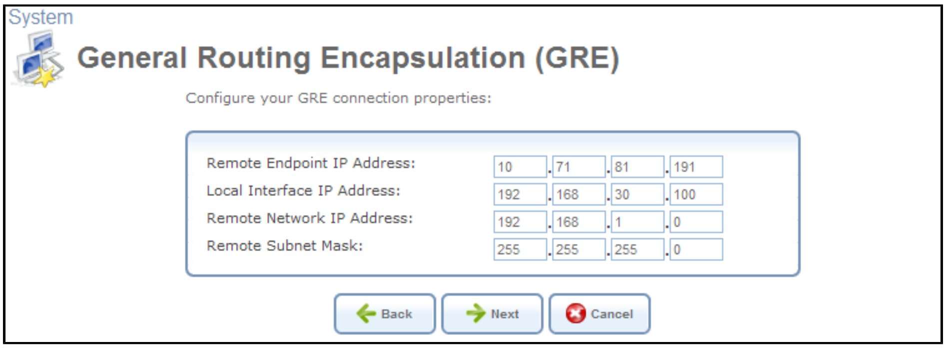


Figure 6.294 General Routing Encapsulation (GRE)

4. Enter 10.71.81.191 as the tunnel's remote endpoint IP address.

5. Enter 192.168.30.100 as the local IP address of this gateway's GRE interface.

6. Enter 192.168.1.0 as the IP address of the remote network that will be accessed via the tunnel, and 255.255.255.0 as the subnet mask. Click 'Next'.

7. In the 'Connection Summary' screen, select the 'Edit the Connection' check box, and click 'Finish'. The 'WAN GRE Properties' screen appears (see Figure 6.285).

8. Click the 'Advanced' sub-tab, and deselect the 'Internet Connection Firewall' check box.

9. Click 'OK' to save the settings.

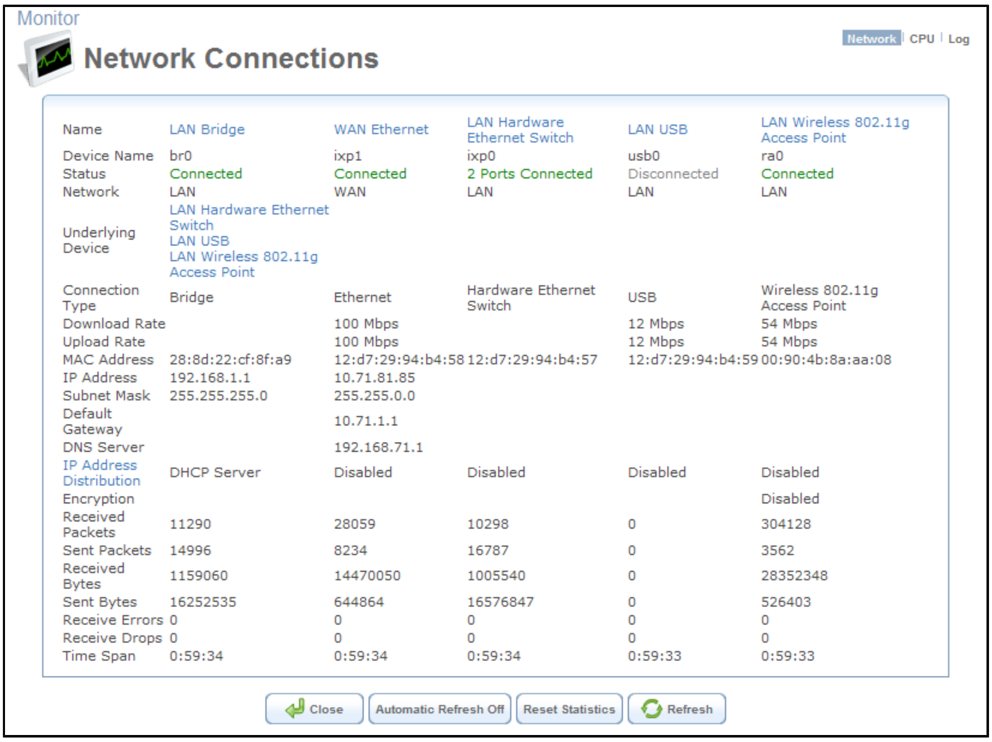
6.4.18.3.5 Running the Scenario

After verifying that each host had properly received an IP address in the subnet of its respective gateway, send a ping from host A (192.168.1.10) to host B (192.168.30.2). If the GRE connection is successful, host B should reply.

6.5 Monitor

6.5.1 Monitoring Your Network Connections

The 'Network Connections' screen displays a table summarizing the monitored connection data (see Figure 6.295). OpenRG constantly monitors traffic within the local network and between the local network and the Internet. You can view statistical information about data received from and transmitted to the Internet (WAN) and to computers in the local network (LAN).



Name	LAN Bridge	WAN Ethernet	LAN Hardware Ethernet Switch	LAN USB	LAN Wireless 802.11g Access Point
Device Name	br0	ixp1	ixp0	usb0	ra0
Status	Connected	Connected	2 Ports Connected	Disconnected	Connected
Network	LAN	WAN	LAN	LAN	LAN
Underlying Device	LAN Hardware Ethernet Switch LAN USB LAN Wireless 802.11g Access Point				
Connection Type	Bridge	Ethernet	Hardware Ethernet Switch	USB	Wireless 802.11g Access Point
Download Rate		100 Mbps		12 Mbps	54 Mbps
Upload Rate		100 Mbps		12 Mbps	54 Mbps
MAC Address	28:8d:22:cf:8f:a9	12:d7:29:94:b4:58	12:d7:29:94:b4:57	12:d7:29:94:b4:59	00:90:4b:8a:aa:08
IP Address	192.168.1.1	10.71.81.85			
Subnet Mask	255.255.255.0	255.255.0.0			
Default Gateway		10.71.1.1			
DNS Server		192.168.71.1			
IP Address Distribution	DHCP Server	Disabled	Disabled	Disabled	Disabled
Encryption					Disabled
Received Packets	11290	28059	10298	0	304128
Sent Packets	14996	8234	16787	0	3562
Received Bytes	1159060	14470050	1005540	0	28352348
Sent Bytes	16252535	644864	16576847	0	526403
Receive Errors	0	0	0	0	0
Receive Drops	0	0	0	0	0
Time Span	0:59:34	0:59:34	0:59:34	0:59:33	0:59:33

Figure 6.295 Monitoring Connections

Click the 'Refresh' button to update the display, or the 'Automatic Refresh On' button to constantly update the displayed parameters.

6.5.2 Monitoring the CPU Load

Click the 'CPU' link in the links bar to view the gateway's CPU status. The 'CPU' screen displays a real-time report about the CPU's status and load.

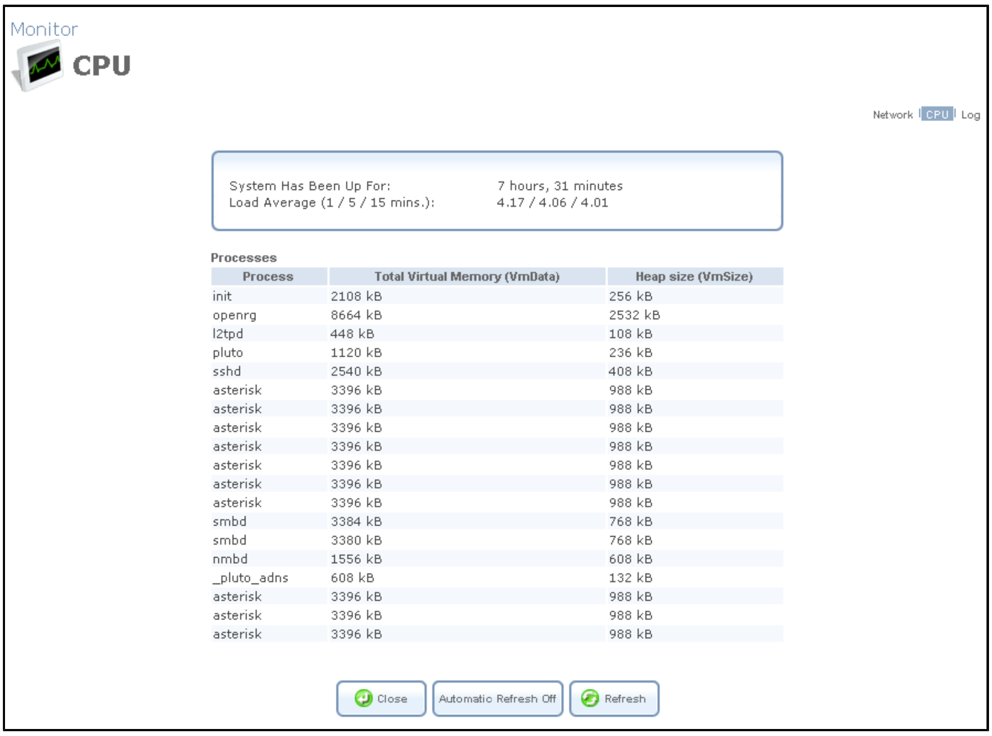


Figure 6.296 CPU Monitoring

- **System Has Been Up For** The amount of time that has passed since the system was last started.
- **Load Average (1 / 5 / 15 mins.)** The average number of processes that are either in a runnable or uninterruptible state. A process in the runnable state is either using the CPU or waiting to use the CPU. A process in the uninterruptible state is waiting for I/O access, e.g. waiting for the disk. The averages are taken over the three time intervals. The meaning of the load average value varies according to the number of CPUs in the system. This means for example, that a load average of 1 on a single-CPU system means that the CPU was loaded all the time, while on a 4-CPU system this means that the CPU was idle 75% of the time.
- **Processes** A list of processes currently running on OpenRG, and their virtual memory usage. The amount of memory granted for each process is presented with the help of the following parameters:
  - **Total Virtual Memory (VmData)** The amount of memory currently utilized by the running process.
  - **Heap size (VmSize)** The total amount of memory allocated for the running process.

Note: Some processes have several child processes. The child processes may be displayed under the same name as the parent one, and use the same memory address space.

This screen is automatically refreshed by default, though you may change this by clicking 'Automatic Refresh Off'.

6.5.3 Viewing the System Log

Click the 'Log' link in the links bar to view your system's log. The 'System Log' screen displays a list of recent activities that has taken place on OpenRG.

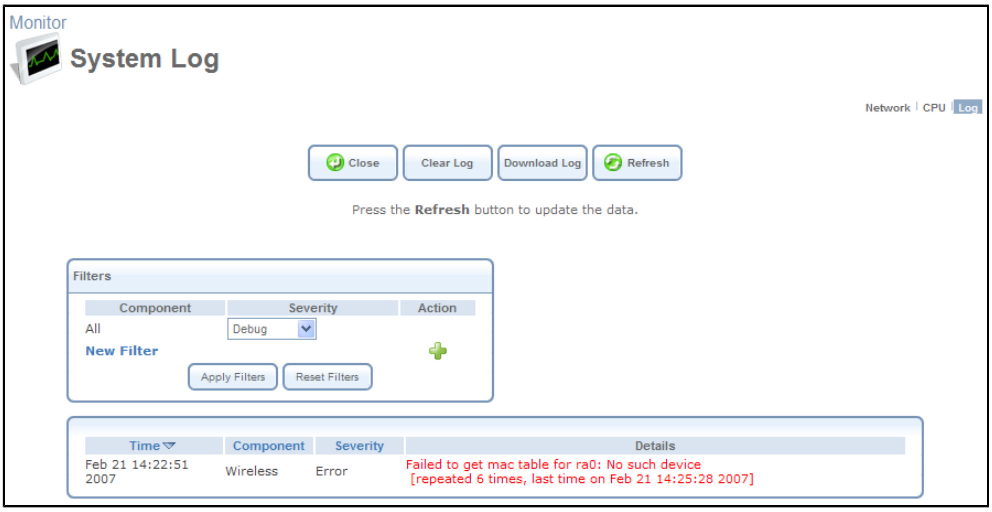


Figure 6.297 System Log

Use the buttons at the top of the page to:

Close Close the 'Log' screen and return to OpenRG's home page.

Clear Log Clear all currently displayed log messages.

Download Log Download the log as a Comma Separated Value (CSV) file, named **openrg_log.csv**.

Refresh Refresh the screen to display the latest updated log messages.

By default, all log messages are displayed one after another, sorted by their order of posting by the system (newest on top). You can sort the messages according to the column titles—Time, Component, or Severity. This screen also enables you to filter the log messages by the component that generated them, or by their severity, providing a more refined list. This ability is useful mainly for software developers debugging OpenRG.

By default, the screen displays log messages with 'debug' severity level and higher, for all components (see default filter in Figure 6.297). You may change the severity level for this filter. To add a new filter, click the 'New Filter' link or its corresponding  action icon . The screen refreshes.

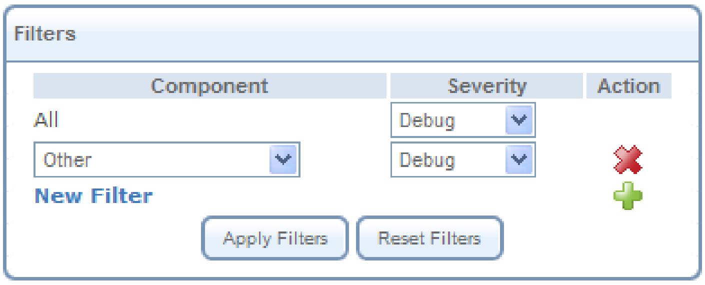


Figure 6.298 System Log Filters

Using the drop-down menus, select the component and severity level by which to sort the log messages. Click 'Apply Filters' to display the messages in your specified criteria. You can add more filters in the same way, or delete filters using their respective action icons. Defined filters override the default filter that displays all messages.

> Note: Clicking "Reset Filters" deletes all the defined filters without a warning.

Note that if you would like to view OpenRG's system log in your host's command prompt, you must install and run the syslog server. Then, configure OpenRG with your host's IP address as described in Section 6.2.

6.6 Routing

6.6.1 Managing the Routing Table

The 'Routing' screen enables you to add, edit, or delete routing rules from OpenRG's routing table.

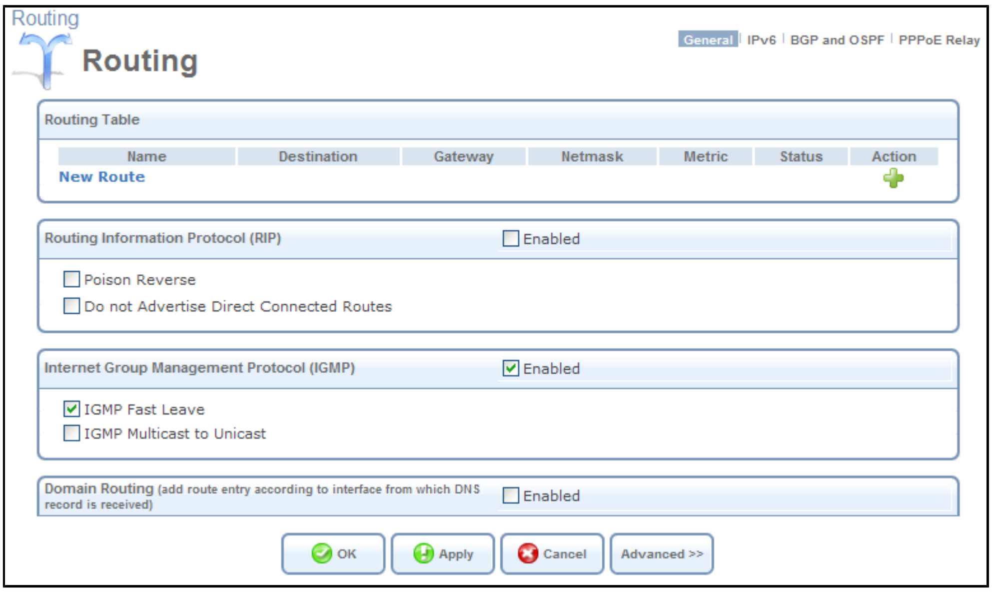


Figure 6.299 Routing

Note that this table only displays routing rules that you define manually using the WBM, and does not display dynamic rules applied by OpenRG's network connection interfaces, such as IPSec, OSPF, RIP, etc..

To view the advanced routing settings, click the 'Advanced' button.

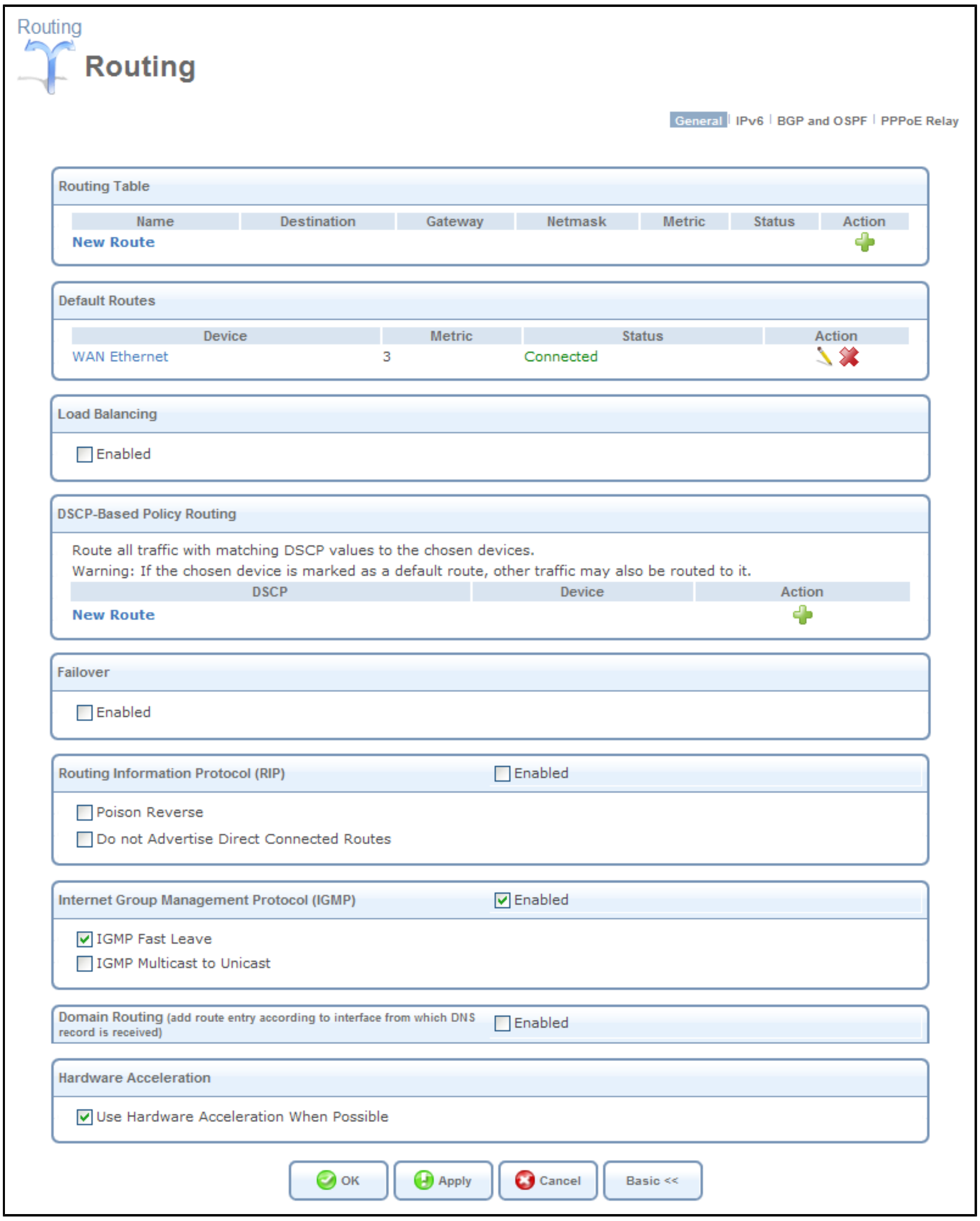


Figure 6.300 Routing – Advanced View

6.6.1.1 Adding a Routing Rule

To add a routing rule, click the 'New Route' link or the  action icon . The 'Route Settings' screen appears.

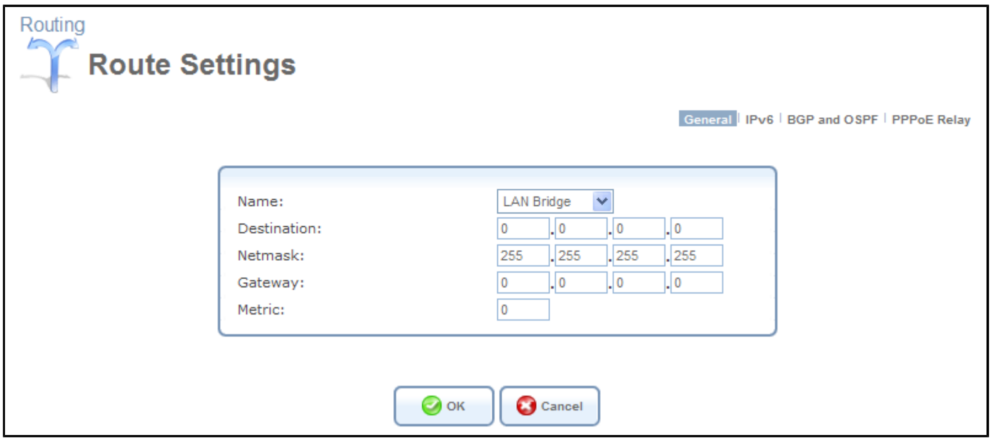


Figure 6.301 Route Settings

Specify the following:

Name Select the network device.

Destination Enter the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.

Netmask The network mask is used in conjunction with the destination to determine when a route is used.

Gateway Enter the gateway's IP address.

Metric A measurement of a route's preference. Typically, the lowest metric is the most preferred route. If multiple routes have the same metric value, the default route will be the first in the order of appearance.

6.6.1.2 Default Routes

OpenRG's default route devices are displayed in the 'Default Routes' section of the 'Routing' screen. You can change the route preference by clicking an entry's action icon and changing the metric value. If you wish to add an additional (logical) default route device, you must first define a new WAN device that has an IP address.

For example:

1. Define a new PPTP VPN connection over your WAN (to learn how to do so, refer to Section 6.4.11.2). The 'New Default Route' link appears in the 'Default Routes' section of the 'Routing' screen.

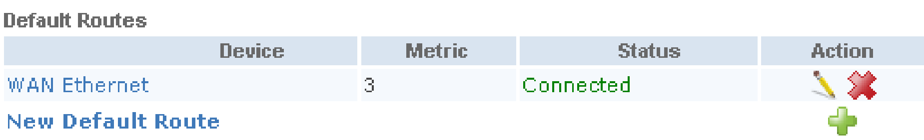


Figure 6.302 Default Routes

2. Click the 'New Default Route' link in the 'Default Routes' section. The 'Default Route Settings' screen appears, displaying the new WAN device.

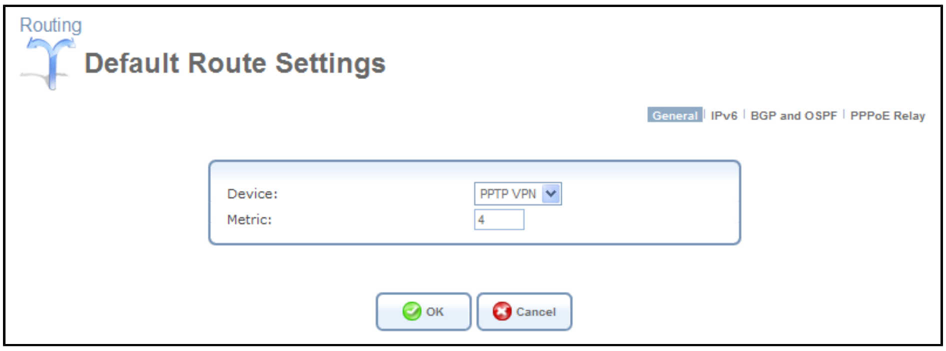


Figure 6.303 Default Route Settings

3. Enter a value for the metric route preference.
4. Click 'OK' to save the settings.

Although multiple devices may be configured as default routes, only one will serve as the default route—the one with the lowest metric value, or, if metric values are identical, the first in order. Defining a single default route is especially important in conjunction with the DSCP-based policy routing (refer to Section 6.6.1.3.2).

6.6.1.3 Multiple WAN Devices

OpenRG supports platforms with multiple physical WAN devices, which can be used for traffic load balancing, failover, and various routing policies. The multiple WAN features may also be used to define multiple logical devices (e.g. PPTP VPN, PPPoE) on boards with a single WAN device.

- **Load balancing** means that you may choose to balance the traffic load between the two WAN devices (refer to Section 6.6.1.3.1).
- **DSCP-based policy routing** means that you may specify that all traffic matching a certain DSCP value will be routed to a chosen device (refer to Section 6.6.1.3.2).
- **Failover** means that traffic will be routed to an active WAN device in case its current WAN device fails, ensuring connectivity (refer to Section 6.6.1.3.3).

Note: DSCP-based policy routing takes precedence over load balancing. In addition, if WAN failover occurs, it will take place on the remaining non-DSCP directed traffic only.

6.6.1.3.1 Load Balancing

Load balancing provides the ability to use the bandwidth of two parallel WAN devices for distributing traffic. Load balancing uses the IP pairs technique, in which traffic between a pair of source and destination IP addresses is routed to the same WAN device for a certain

timeframe. A router load balancing on a per-destination basis uses the parallel routes in a round-robin fashion, and forwards an entire destination-based flow in each pass.

> Note: Only default route devices (refer to Section 6.6.1.2) can participate in load balancing.

To enable load balancing between multiple WAN devices, perform the following:

1. Select the 'Enabled' check box in the 'Routing' screen (see Figure 6.300). The screen refreshes, displaying the load balancing table.

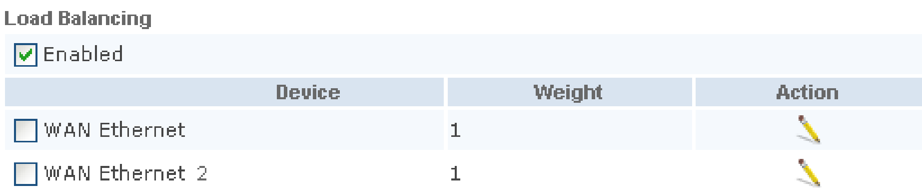


Figure 6.304 Load Balancing

2. Select the devices on which load balancing will be performed by selecting their respective check boxes.

3. You may also control the weight of each device in the balancing procedure, which determines the ratio of IP pairs provided to each device:

   a. Click the action icon of the device. The 'Edit Weight of Device' screen appears.

   Figure 6.305 Edit Weight of Device

   b. Enter the numeric ratio that will represent the weight of the device.

   c. Click 'OK' to save the settings.

4. Click 'OK' to save the settings.

6.6.1.3.2 DSCP-Based Policy Routing

DSCP-based policy routing provides the ability to send specific traffic out of a specific WAN device. This is useful for routing different types of data to different WAN devices. It is also

useful if you would like to segregate the voice traffic from the data traffic over two lower-cost broadband circuits in an effort to have better voice quality.

To add a DSCP-based policy route, perform the following:

1. Click the 'New Route' link. The 'Add a DSCP-Based Route to a Device' screen appears.

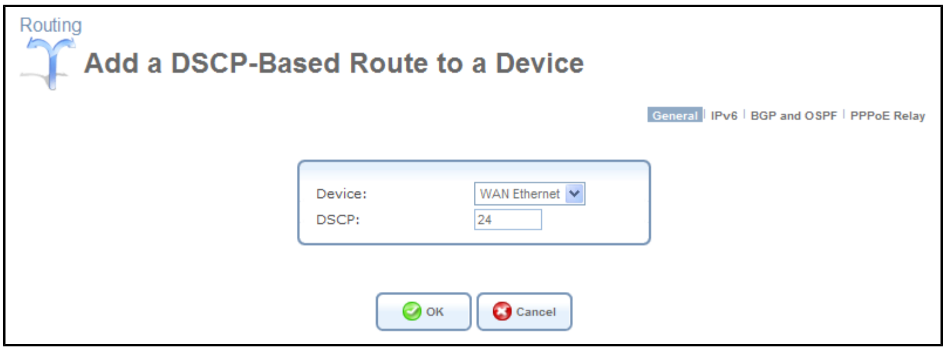


Figure 6.306 Adding a DSCP-Based Route to a Device

2. Select the network device from the drop-down menu.

3. Specify the DSCP value. All traffic matching this DSCP value will be routed to the chosen device.

4. Click 'OK' to save the settings.

You can mark certain traffic with DSCP values of your choice, as explained in Section 6.4.16.2.4). The DSCP-based policy routing ensures that specified traffic is routed via a certain WAN device, but if this WAN device is defined as the default route, other traffic may also be routed through it. If you want your device to be dedicated to transmitting only traffic matching the DSCP value you specified, you must deselect the default route check box for that device.

DSCP-based policy routing takes precedence over load balancing, so if most of the traffic falls under the DSCP-based policy routing rules, it will be forwarded accordingly, regardless of the load balancing. Load balancing, in this case, will be a best-effort load balancing, and will balance the remaining traffic not directed by the DSCP-based policy routing rules.

6.6.1.3.3 Failover

Failover is the transfer of operation from a failed device to a similar, reserved device to ensure uninterrupted data flow and operability. OpenRG supports WAN failover on multiple WAN platforms.

WAN failover takes place when a WAN device fails due to disconnection or an unsuccessful DNS test. This means that if the WAN Ethernet 1 device fails, its routing rules are removed, and all traffic will now be routed through WAN Ethernet 2 according to its routing scheme, until WAN Ethernet 1 resumes its connectivity. It is recommended to use this feature in conjunction with default route rules defined on both devices.

OpenRG supports the following types of failover:

- **Full Link Redundancy** Two or more active WAN devices, usually with equal speed, must be configured. During normal operation, traffic is routed through them according to route rules, or load balancing. If one of the devices fails, the next one will take its place.
- **Rollover Connection** During uptime, a rollover device is kept inactive. This is usually a slow link, for example, a dialup. When all other failover devices lose connectivity, the rollover device will become active automatically, and may keep the same IP as the main device. This allows to use a slow connection as a backup to the main fast connection. When a failed device regains connectivity, the rollover device will become inactive again. Note that if dialup is done by demand, activating the backup device may take a noticeable amount of time.

The failover process consists of three phases:

1. **Detection** – performed using a DNS test.
2. **Action** – when a DNS test fails, the failover process simply removes the route records of the failed connection. This enables you to reach the desired failover behavior by configuring OpenRG's routing rules correctly.
3. **Recover** – during failover, tests continue to run on the failed connection. When a test succeeds, the connection will recover its route records.

Failover scenarios:

- **Inbound Failover** A common problem occurs when a connection fails, and its IP is no longer accessible. This is referred to as Inbound Failover, and is resolved by informing the other party to use a different IP, using Dynamic DNS.
- **IPSec** (Also, refer to Section 5.8.1.3) When an IPSec underlying connection loses connectivity or fails connectivity tests, the following scenarios are possible:
    1. In case an IPSec template is available, traffic will be received from all WAN devices.
    2. In case an IPSec connection is defined, and:
        a. No underlying connection is configured—the IPSec connection will disconnect and attempt to reconnect while choosing the underlying connection according to existing route rules.
        b. An underlying connection is configured—the behavior will be similar, with the exception that the chosen underlying connection may only be a failover connection to the configured underlying connection. If you wish to force IPSec to use the configured underlying connection without failover, do not configure the underlying connection as a failover connection.
    3. At the recover stage, if:

a. No underlying connection is configured—OpenRG assumes that the WAN connection used as the underlying connection is unimportant. Hence, the IPSec connection will not disconnect from its current device.

b. An underlying connection is configured—the IPSec connection will always try to go back to its configured underlying device. It will disconnect, and return to the recovered WAN connection.

To enable failover between multiple WAN devices, perform the following:

1. Select the 'Enabled' check box in the 'Routing' screen (see Figure 6.300). The screen refreshes, displaying the failover table.

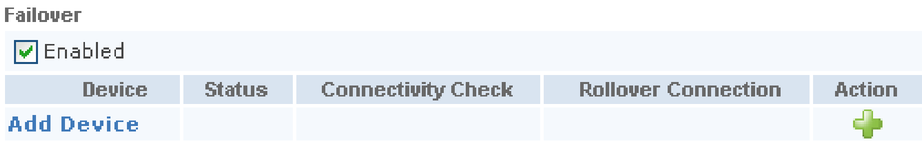


Figure 6.307 Failover

2. Click the 'Add Device' link to add a failover device. The 'Add Failover Device' screen appears.

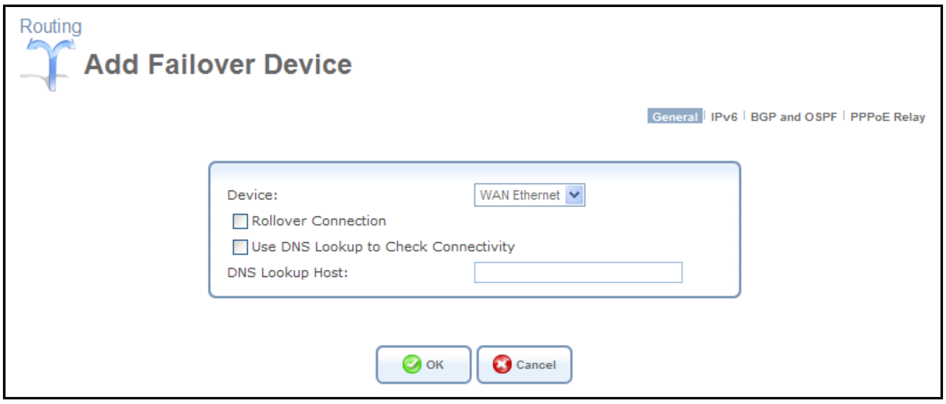


Figure 6.308 Add Failover Device

Device Select the WAN device you would like to configure as failover.

Rollover Connection Select this check box to configure the WAN device as a rollover connection type of failover.

Use DNS Lookup to Check Connectivity Select this check box to enable a periodic connectivity check using a DNS query.

DNS Lookup Host If you selected the previous check box, enter the URL that the periodic check will query.

3. Click 'OK' to save the settings.

In order to clarify the use of failover, following are failover use-cases that depict actual uses of this feature. These use-cases assume that you are running a multiple WAN platform with at least two WAN devices.

- **Redundancy** In the 'Routing' screen (see Figure 6.300), perform the following steps:

  1. In the 'Default Routes' section, define WAN Ethernet (WAN 1) as a default route with metric 3.

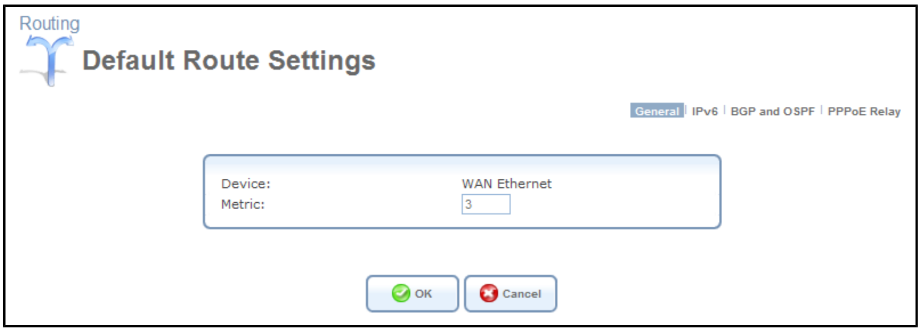


Figure 6.309 WAN 1 Default Route Settings

  2. Similarly, define WAN Ethernet 2 (WAN 2) as a default route with metric 5.

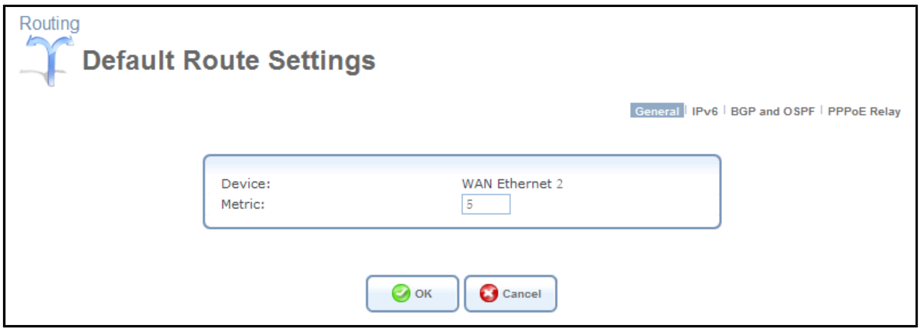


Figure 6.310 WAN 2 Default Route Settings

  3. In the 'Routing Table' section, click the 'New Route' link to define a route rule for WAN 2, with destination 192.168.71.0, netmask 255.255.255.0, and gateway 192.168.71.1.

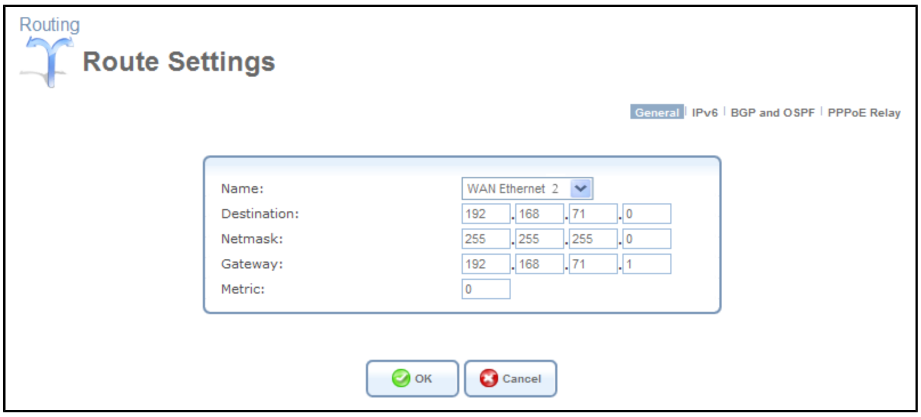


Figure 6.311 WAN 2 Route Rule

4. In the 'Failover' section, add both devices to the failover table, defining them with DNS connectivity checks set to http://www.google.com.

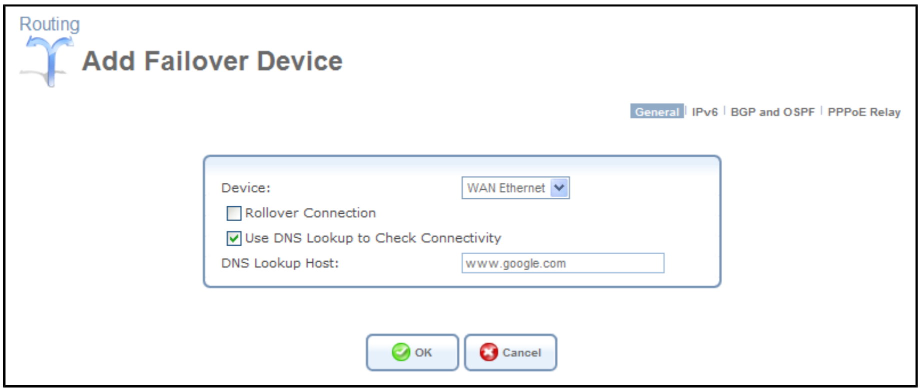


Figure 6.312 Add Failover Device

5. Click 'OK' to save the settings.

When both connections are active, the default route will be WAN 1, while WAN 2 will be used merely for access to destination 192.168.71.0. If WAN 1 fails, its route records will be deleted, and WAN 2 will become the default route, handling all traffic.

- **Full Link Redundancy with Load Balancing** This use-case is similar to the previous one, but with load balancing between the default routes.

1. Define all settings according to the previous use-case.

2. In the 'Load Balancing' section, select the check boxes of both WAN 1 and WAN 2.

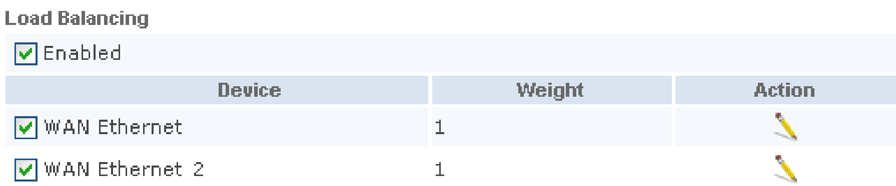


Figure 6.313 Load Balancing

3. Click 'OK' to save the settings.

When both connections are active, both will share the traffic, except for traffic to 192.168.71.0, which will only be redirected to WAN 2. If one of the devices fails, the other will instantly take responsibility over all traffic.

- **Rollover**

1. In the 'Default Routes' section, click the 'New Default Route' link to define WAN 1 as a default route with metric 3.

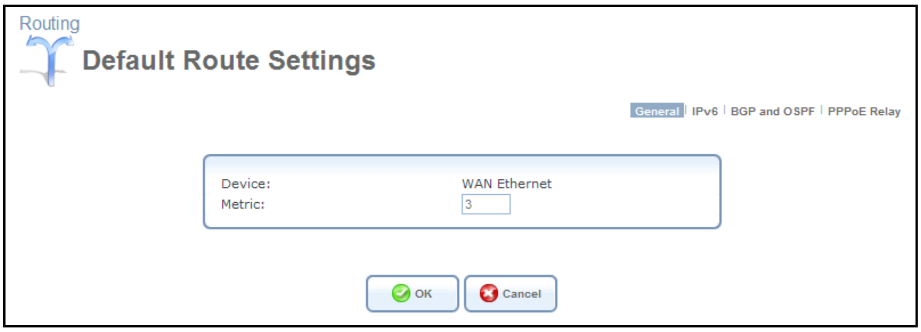


Figure 6.314 WAN 1 Default Route Settings

2. Similarly, define WAN 2 as a default route with metric 3.

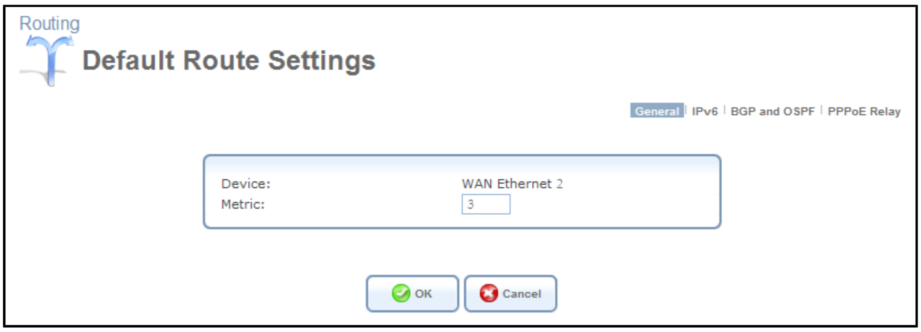


Figure 6.315 WAN 2 Default Route Settings

3. In the 'Routing Table' section, click the 'New Route' link to define a route rule for WAN 1, with destination 192.168.71.0, netmask 255.255.255.0, and gateway 192.168.71.1.

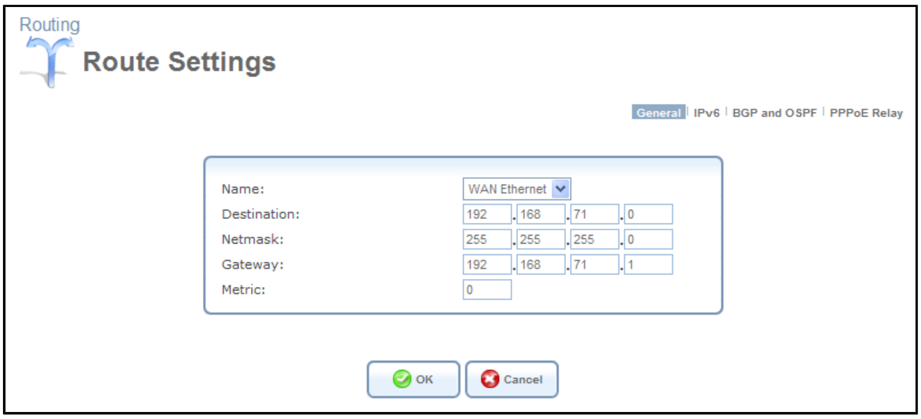


Figure 6.316 WAN 1 Route Rule

4. In the 'Failover' section, add WAN 1 to the failover table, defining it with a DNS connectivity check set to http://www.google.com.

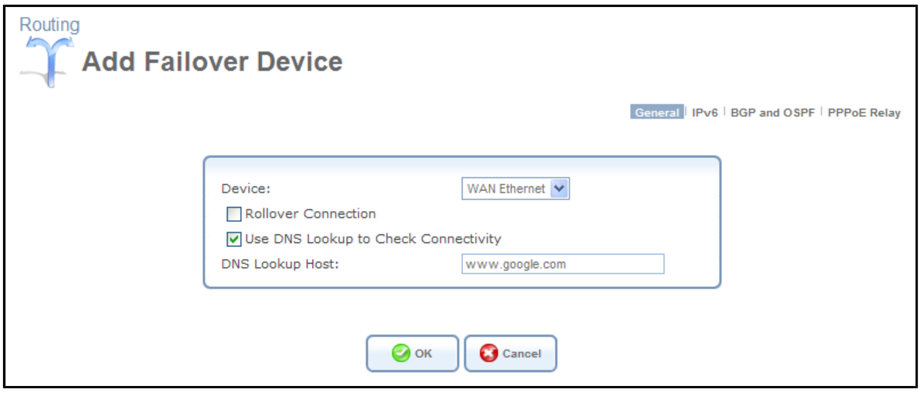


Figure 6.317 WAN 1 Failover Settings

5. Similarly, add WAN 2, defining it as a rollover connection.

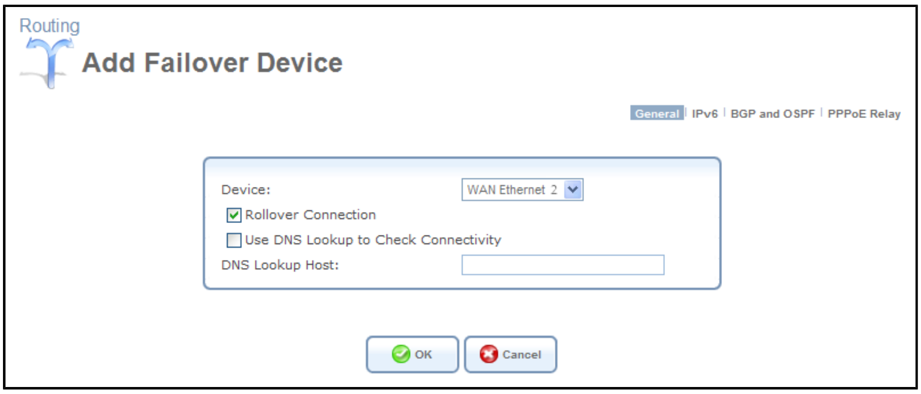


Figure 6.318 WAN 2 Failover Settings

6. Click 'OK' to save the settings.

Regularly, only WAN 1 will be active, handling all traffic, while WAN 2 is dormant. If WAN 1 fails, WAN 2 will become active. In case WAN 2 is a dialup device, it will start a dialup session with the ISP. After establishing a connection, it will become the default route, since its default route record is the only one remaining active. Should WAN 1 become active again, WAN 2 will recognize that it is no longer needed, and will shut down.

6.6.1.4 Supported Routing Protocols

Routing Information Protocol (RIP) Select this check box in order to enable connections previously defined to use RIP. If this check box is not selected, RIP will be disabled for all connections, including those defined to use RIP.

- **Poison Reverse** OpenRG will advertise acquired route information with a high metric, in order for other routers to disregard it.
- **Do not Advertise Direct Connected Routes** OpenRG will not advertise the route information to the same subnet device from which it was obtained.

Internet Group Management Protocol (IGMP) OpenRG provides support for the IGMP multicasting. When a host sends out a request to join a multicast group, OpenRG will listen and intercept the group's traffic, forwarding it to the subscribed host. OpenRG keeps record of subscribed hosts. When a host requests to cancel its subscription, OpenRG queries for other subscribers and stops forwarding the multicast group's traffic after a short timeout.

- **Enable IGMP Fast Leave** If a host is the only subscriber, OpenRG will stop forwarding traffic to it immediately upon request (there will be no query delay).
- **IGMP Multicast to Unicast** Enables OpenRG to convert the incoming multicast data stream into unicast format, in order to route it to the specific LAN host that had requested the data. In this way, OpenRG will prevent flooding the rest of the LAN hosts with irrelevant multicast traffic.

Domain Routing When OpenRG's DNS server receives a reply from an external DNS server, it will add a routing entry for the IP address of the reply through the device from which it arrived. This means that future packets from this IP address will be routed through the device from which the reply arrived.

6.6.1.5 Hardware Acceleration

The Hardware Acceleration feature utilizes the **Fastpath** algorithm, which enhances packet flow, resulting in faster communication between the LAN and the WAN (excluding the wireless connection). By default, this feature is enabled.

6.6.2 IPv6

At the current stage of the IP network technology, an IPv4 WAN has no inherent support of Internet Protocol version 6 (IPv6). As a result, two IPv6 hosts cannot communicate with each other directly, if they are located at two separate IPv6 LANs interconnected by an IPv4 WAN (either the global Internet or a corporate WAN).

The easiest way to solve this problem is to establish a special network mechanism, called *IPv6-over-IPv4 Tunneling*. This mechanism encapsulates IPv6 packets into IPv4 packets, in order to transmit them via an IPv4 WAN to the target IPv6 host. OpenRG successfully implements the IPv6 technology.

The following scenario demonstrates how to establish communication between two IPv6 hosts via OpenRG. Each host belongs to a separate IPv6 network. The two networks are interconnected by an IPv4 WAN. For convenience, let's call the two machines Host **A** and Host **B**. In the same fashion, let's call the two gateways, connected to the host machines, OpenRG **A** and OpenRG **B** respectively.

The following diagram outlines this scenario.

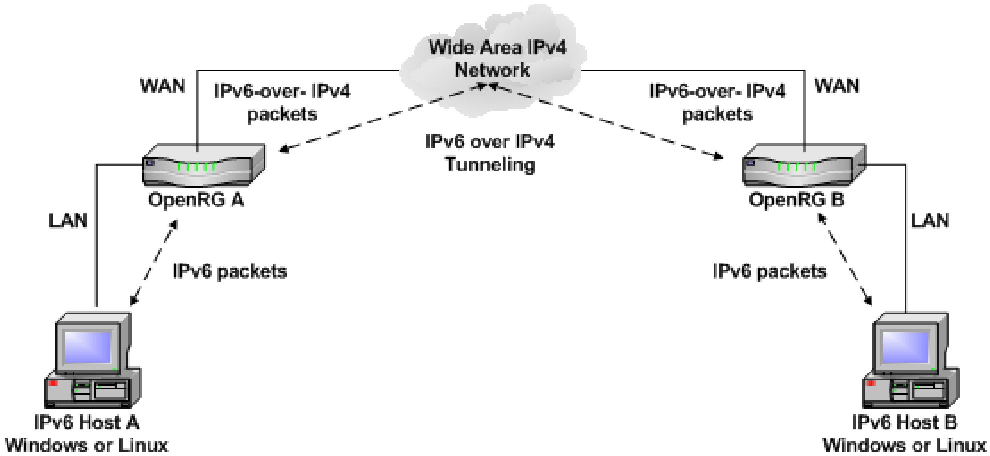


Figure 6.319 IPv6-over-IPv4 Tunneling via OpenRG

There are several variations of the IPv6 network setup, depending on the operating system installed on the host machines. OpenRG's IPv6 feature enables you to establish an IPv6 network between:

- Linux hosts
- Windows hosts
- Linux and Windows hosts

> Note: The following instructions should be followed at both ends of the IPv6- over-IPv4 tunnel, otherwise the packets will travel only in a single direction.

After connecting the IPv6 hosts to their gateways at both locations, perform the following:

1. Configure the gateways to support the IPv6-over-IPv4 tunneling.
2. Configure the IPv6 hosts according to the parameters defined in their gateways.

The following sections describe each of these steps.

6.6.2.1 Setting up the IPv6-over-IPv4 Tunneling in OpenRG

This setup procedure consists of the following steps:

- Enabling the IPv6 feature
- Adding a new LAN subnet to the LAN bridge and configuring its settings
- Configuring the IPv6-over-IPv4 tunnel settings

1. Verify that the IPv6 feature is enabled in each of the gateways, by performing the following:

a. Click the 'IPv6' icon in the 'Advanced' screen of the WBM. If the feature is disabled, the following screen appears.

Figure 6.320 Disabled IPv6

b. Select the 'Enabled' check box. The screen refreshes, changing to the following.

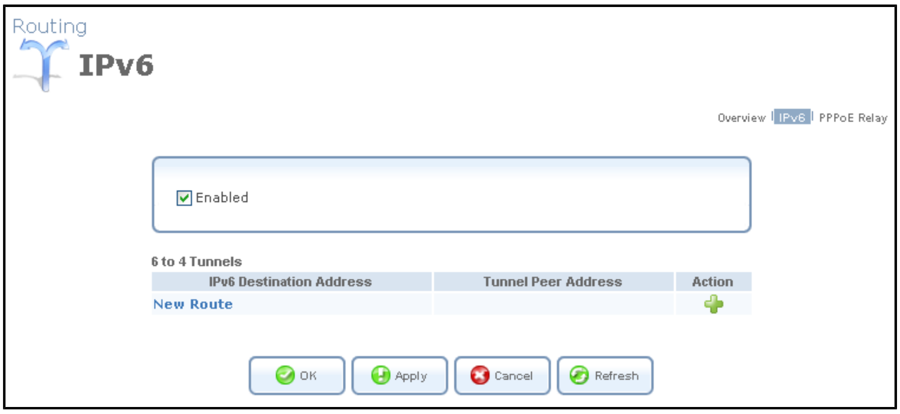


Figure 6.321 Enabled IPv6

c. Click 'Apply' to save the settings.

2. Add a new LAN subnet to the LAN bridge by performing the following:

a. Under the 'System' tab, click the 'Network Connections' menu item. The 'Network Connections' screen appears.

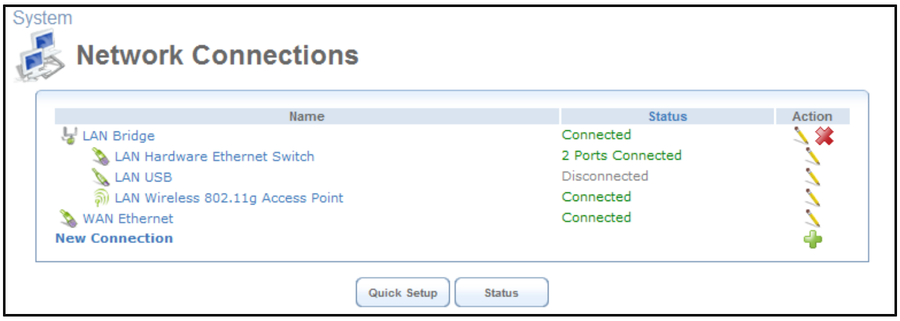


Figure 6.322 Network Connections

b. Click the 'LAN Bridge' link. The 'LAN Bridge Properties' screen appears.

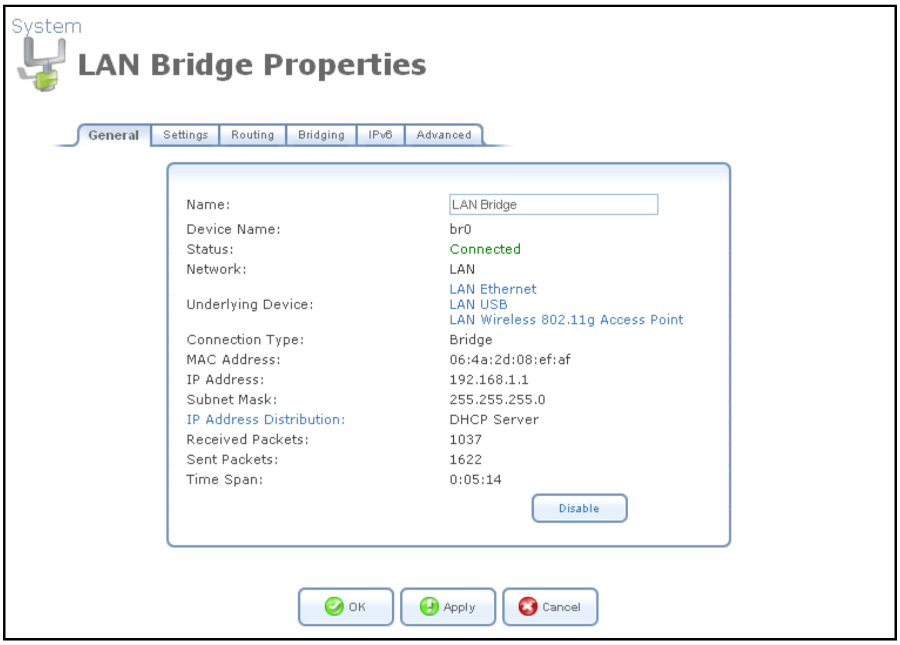


Figure 6.323 LAN Bridge Properties

c. Click the 'IPv6' link. The IPv6 settings screen appears.

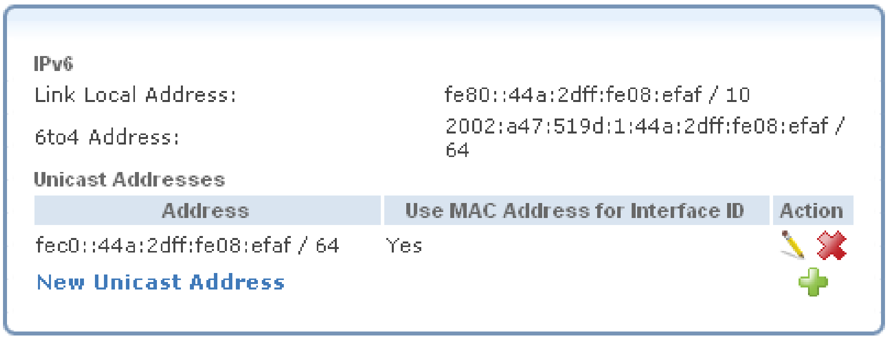


Figure 6.324 IPv6 Settings

d. Click the 'New Unicast Address' link. Alternatively, click its action icon . The 'IPv6 Unicast Address' screen appears.

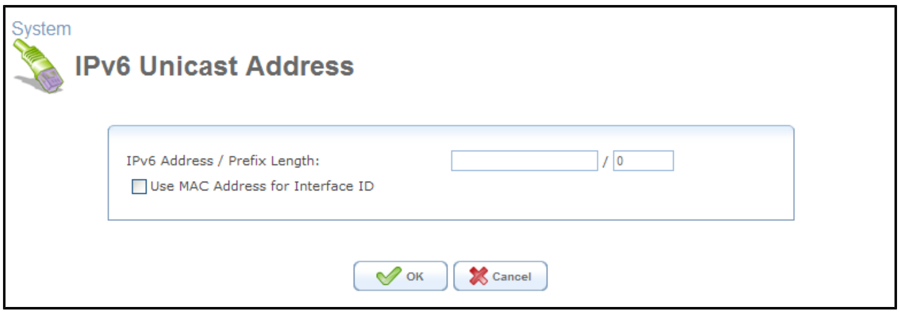


Figure 6.325 IPv6 Unicast Address Parameters

e. In the 'IPv6 Address/Prefix Length' field, enter the IPv6 address of the new LAN subnet and its prefix length. For example, assign the following IPv6 address to the LAN subnet of OpenRG **A**: `fec0::100:aaaa:bbbb:cccc:dddd/64`

   The `fec0` part shows that this is a *Site-Local* address (an IPv6 address within a LAN). The `100` part is the ID number of the subnet. The next four parts (represented with letters) are unrestricted, unless they are generated from the gateway's MAC address. The `64` part is the prefix length.

> Note: The 'IPv6 Unicast Address' screen contains the 'Use MAC Address for Interface ID' option. If it is enabled, OpenRG generates the lower 64 bits of the IPv6 address from its MAC address.

f. Click 'OK' to save the setting, and to return to the 'LAN Bridge Properties' screen.

g. Verify that the new subnet has received the unicast address.

In the same way as described above, define a new subnet in OpenRG **B**. For example, assign the following IPv6 address to this subnet: `fec0::200:aaaa:bbbb:cccc:dddd/64`

3. Configure the IPv6-over-IPv4 tunnel in **each of the gateways**. For example, to configure the tunnel in OpenRG **A**, perform the following:

   a. In the 'IPv6' settings screen (see Figure 6.321), click the 'New Route' link to specify the IPv6-over-IPv4 tunnel parameters. The 'Set IPv6 Tunnel' screen appears.

Figure 6.326 IPv6 Tunnel Parameters

   b. In the 'IPv6 Destination Address/Prefix Length' field, specify the IPv6 address of the OpenRG **B** LAN subnet.

   c. In the 'Tunnel Peer IP Address' fields, enter the WAN IP of OpenRG **B**.

   d. Click 'OK' to save the settings.

In the same fashion, configure OpenRG **B**.

6.6.2.2 Setting up the IPv6 Network Connection on a Linux Host

This setup procedure consists of the following steps:

- Adding IPv6 support, if not yet enabled
- Adding the new LAN subnet defined in OpenRG
- Creating an IPv6 routing rule

1. Verify that the Linux host supports IPv6, by performing the following:

   a. Open a shell and switch to the root user, by entering the `su` command.

   b. Enter the following command:

   ```
   lsmod | grep ipv6
   ```

   If the command returns no result, it means that IPv6 support is disabled. To enable IPv6 support, enter the following command as the root user:

   ```
   insmod ipv6
   ```

2. Add the IPv6 address defined in the new LAN subnet to the host's network settings. For example, assign the IPv6 address of the OpenRG **A** LAN subnet to the Host **A** network device. To do so, run the following command as the root user:

   ```
   ip -6 addr add fec0::100:1111:2222:3333:4444/64 dev <Host A LAN connection label>
   ```

   > Note: To check the network connection label in Linux, run the `ifconfig` command.

   If Host **B** runs Linux too, follow the procedure described above. In this case, however, you must specify the IPv6 address defined in the OpenRG **B** LAN subnet, and enter the network connection label of the Host **B** machine.

3. Add a routing rule directing the host's outgoing IPv6 packets to OpenRG, which will route them to the destination. For example, to add this routing rule to the network settings of Host **A**, run the following command as the root user:

   ```
   ip -6 route add fec0::200:1111:2222:3333:4444/64 via fec0::100:aaaa:bbbb:cccc:dddd
   dev <Host A LAN connection label>
   ```

   If Host **B** runs Linux too, go to its shell and run the following command as the root user:

   ```
   ip -6 route add fec0:0:0:100:1111:2222:3333:4444/64 via fec0::200:aaaa:bbbb:cccc:dddd
   dev <Host B LAN connection label>
   ```

To test the connection, ping through the IPv6-over-IPv4 tunnel.

- In Linux Host **A** run:

  ```
  ping6 -I <LAN connection label> fec0::200:1111:2222:3333:4444
  ```

- In Linux Host **B** run:

```
ping6 -I <LAN connection label> fec0::100:1111:2222:3333:4444
```

The following are additional commands for testing the IPv6 connection:

- To show the IPv6 routing table, enter:

```
ip -6 route
```

- To show the network device's IPv6 address, enter:

```
ip -6 addr
```

If the second host runs Windows, refer to Section 6.6.2.3 for explanations about configuring a Windows host.

6.6.2.3 Setting up the IPv6 Network Connection on a Windows Host

This setup procedure consists of three steps:

- Adding IPv6 support, if not yet enabled
- Adding the new LAN subnet defined in OpenRG
- Creating an IPv6 routing rule

> Note: The following description is based on the GUI of Windows XP. For information about installing IPv6 on other Windows versions, visit the Microsoft Web site.

1. Verify that the host running Windows supports IPv6, by performing the following:

   a. In 'Control Panel', double-click the 'Network Connections' icon. The 'Network Connections' window appears.

   b. In the 'Network Connections' window, right-click the network connection label (the default label is 'Local Area Connection') and select 'Properties'. The following window appears.

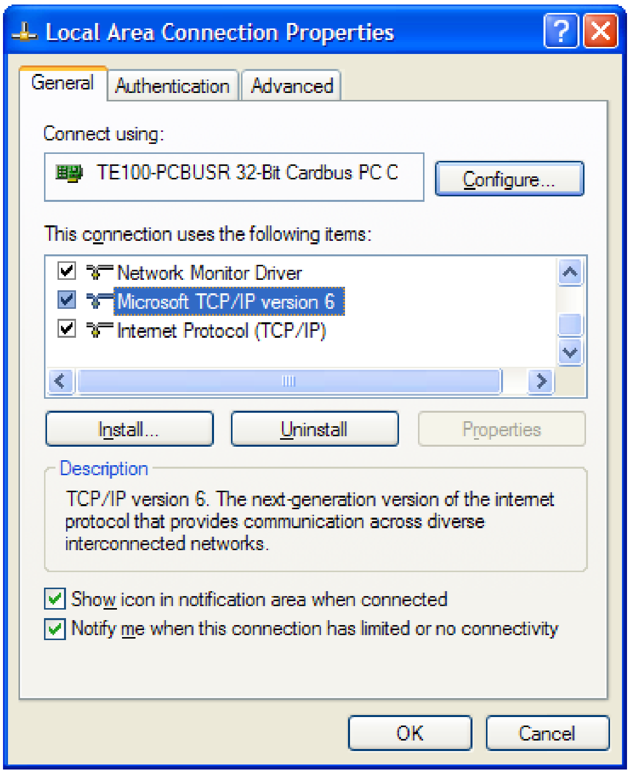


Figure 6.327 Network Connection Properties

c. Ensure that the 'General' tab is selected, and check if the list of connection options contains the following item: 'Microsoft TCP/IP version 6'. If the list contains this item (IPv6 is installed), verify that its check box is selected and proceed to the next step. Otherwise, install IPv6:

   i. In the 'Start' menu, select 'Run'. The 'Run' window appears.

   ii. In the 'Open' field, enter `cmd` and click 'OK'. The command prompt window appears.

   iii. In the command prompt window, enter the following command:

```
ipv6 install
```

   The command initiates the Microsoft TCP/IP version 6 installation. This is an automatic process.

2. Add the IPv6 address of the new LAN subnet to the host's network settings. For example, assign the IPv6 address of the OpenRG **A** LAN subnet to the Host **A** network device, by performing the following:

   a. In the command prompt window, run the following command:

```
netsh
```

   Netsh is a command-line scripting utility that enables you to modify your computer network configuration.

b. In the `netsh` context, run the following command:

```
interface ipv6
```

c. In the `interface ipv6` context, run the following command:

```
add "<Host A LAN connection label>" fec0::100:1111:2222:3333:4444
```

> Note: The default LAN connection label in Windows is 'Local Area Connection'.

d. Enter the following command:

```
add route fec0::100:aaaa:bbbb:cccc:dddd/64 "<Host A LAN connection label>"
```

If Host **B** runs Windows too, follow the procedure described above, with the only difference that you must specify the IPv6 address of the OpenRG **B** LAN subnet.

3. Add a routing rule directing the host's outgoing IPv6 packets to OpenRG, which will route them to the destination. For example, to add this routing rule to the network settings of Host **A**, run the following command in the 'interface ipv6' context:

```
add route fec0::200:1111:2222:3333:4444/64 interface=<Host A LAN connection label>
nexthop=fec0::100:aaaa:bbbb:cccc:dddd
```

If Host **B** runs Windows too, run the following command in the 'interface ipv6' context:

```
add route fec0::100:1111:2222:3333:4444/64 interface=<Host B LAN connection label>
nexthop=fec0::200:aaaa:bbbb:cccc:dddd
```

To ping through the IPv6-over-IPv4 tunnel, run the following command:

```
ping6 fec0::200:1111:2222:3333:4444/64
```

If the second host runs Linux, refer to Section 6.6.2.2 for explanations about configuring a Linux host.

6.6.3 BGP and OSPF

The 'BGP and OSPF' feature is an implementation of two routing protocols used to deliver up-to-date routing information to a network or a group of networks, called *Autonomous System*.

Border Gateway Protocol (BGP) The main routing protocol of the Internet. It is used to distribute routing information among Autonomous Systems (for more information, refer to the protocol's RFC at http://www.ietf.org/rfc/rfc1771.txt).

Open Shortest Path First Protocol (OSPF) An Interior Gateway Protocol (IGP) used to distribute routing information within a single Autonomous System (for more information, refer to the protocol's RFC at http://www.ietf.org/rfc/rfc2328.txt).
The feature's routing engine is based on the *Quagga* GNU routing software package. By using the BGP and OSPF protocols, this routing engine enables OpenRG to exchange routing information with other routers within and outside an Autonomous System. To enable this feature, perform the following:

1. In the 'Routing' screen, click the 'BGP and OSPF' link. The 'BGP and OSPF' screen appears.

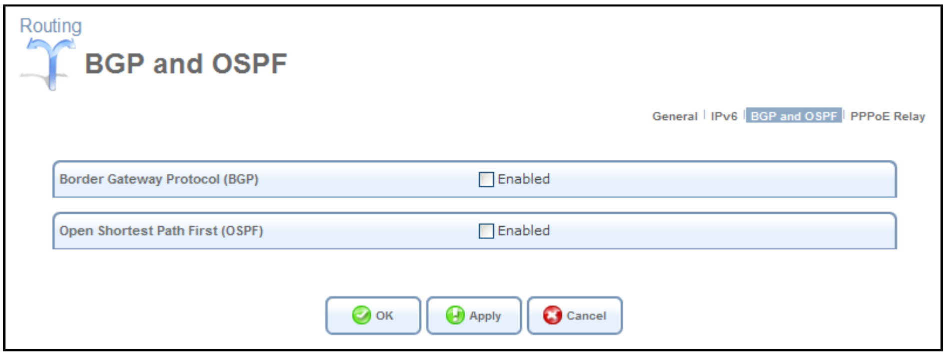


Figure 6.328 BGP and OSPF

Note: Depending on its purpose of use, OpenRG may support both of the protocols or only one of them.

2. Select the 'Enabled' check box of the supported protocol(s). For example, enable OSPF. The screen refreshes, changing to the following.

Figure 6.329 Enabled OSPF

To activate the routing engine, you need to create a configuration file for the protocol daemon, and also for *Zebra*. Zebra is Quagga's IP routing management daemon, which provides kernel routing table updates, interface lookups, and redistribution of routes between the routing protocols.

Note: To view examples of the configuration files, browse to http://www.quagga.net/docs/quagga.pdf.

3. Enter the configuration files into their respective code fields. Alternatively, click the 'Set Default Values' button to the right of each code field. The default values, displayed in a field are the following:

    - **BGP** :

      !router bgp <AS number> The exclamation mark is Quagga's comment character. The `router bgp` string is a command that activates the BGP daemon. The exclamation mark emphasizes that the command must be followed by an exact Autonomous System's ID number.

      log syslog A command that instructs the daemon to send its log messages to the system log.

    - **OSPF** :

      router ospf A command that activates the OSPF daemon.

      log syslog See the explanation under BGP.

    - **Zebra**

      interface ixp1 Instructs the daemon to query and update routing information via a specific WAN device. It is important that you change the default `ixp1` value to your WAN device name.

      log syslog See the explanation under BGP.

4. Click 'OK' to save the settings.

If the OSPF daemon is activated, OpenRG starts sending the 'Hello' packets to other routers to create adjacencies. After determining the shortest path to each of the neighboring routers, Zebra updates the routing table according to the network changes. If the BGP deamon is activated, OpenRG starts to advertise routes it uses to other BGP-enabled network devices located in the neighboring Autonomous System(s). The BGP protocol uses TCP as its transport protocol. Therefore, OpenRG first establishes a TCP connection to routers with which it will communicate. *KeepAlive* messages are sent periodically to ensure the liveness of the connection. When a change in the routing table occurs, OpenRG advertises an *Update* message to its peers. This update message adds a new route or removes the unfeasible one from their routing table.

6.6.4 Enabling PPPoE Relay

PPPoE Relay enables OpenRG to relay packets on PPPoE connections, while keeping its designated functionality for any additional connections. The PPPoE Relay screen (see Figure 6.330) displays a check-box that enables PPPoE Relay.

Figure 6.330 PPPoE Relay

6.7 Performing Advanced Management Operations

6.7.1 Utilizing OpenRG's Universal Plug and Play Capabilities

Universal Plug-and-Play (UPnP) is a networking technology that provides compatibility among networking equipment, software, and peripherals. This technology leverages existing standards and technologies, including TCP/IP, HTTP 1.1 and XML, facilitating the incorporation of Universal Plug-and-Play capabilities into a wide range of networked products for the home.

Your gateway is at the forefront of this technology, offering a complete software platform for UPnP devices. This means that any UPnP-enabled LAN device can dynamically join your network, obtain an IP address, and exchange information about its capabilities and those of other devices on your home network. All this happens automatically, providing a truly zero-configuration network.

The most widespread and trivial example of utilizing OpenRG's UPnP feature is connecting a PC to OpenRG. If your PC is running an operating system that supports UPnP, such as Windows XP™, you will only need to connect it to one of the gateway's LAN sockets. The PC is automatically recognized and added to the local network.

Likewise, you can add any other UPnP-enabled device (for example, a media streamer, digital picture frame, etc.) to your home network.

6.7.1.1 Configuring OpenRG's UPnP Settings

OpenRG's UPnP feature is enabled by default. You can access the UPnP settings from the 'Management' menu item, by clicking the 'Universal Plug and Play' link, or by clicking the 'Universal Plug and Play' icon in the 'Advanced' screen. The 'Universal Plug and Play' settings screen appears.

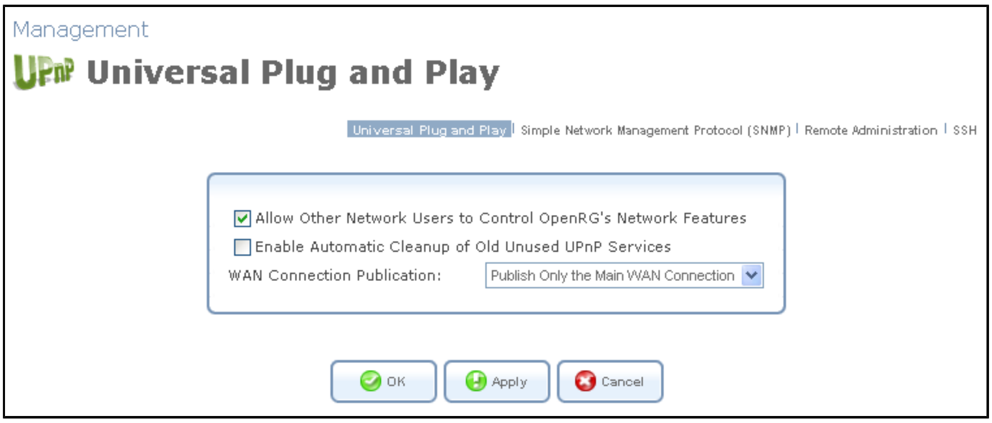


Figure 6.331 Universal Plug and Play

Allow Other Network Users to Control OpenRG's Network Features Selecting this check-box enables the UPnP feature. This will allow you to define local services on any of the LAN hosts, and to make the services available to computers on the Internet, as described in Section 6.7.1.2.

Enable Automatic Cleanup of Old Unused UPnP Services When this check box is selected, OpenRG periodically checks the availability of the LAN computers that have been configured to provide the local services. In case the DHCP lease granted to such a host has expired and the host does not appear in the ARP table, OpenRG removes the port forwarding rule that enables access to the corresponding local service (for more information about port forwarding rules, refer to Section 5.2.3).

WAN Connection Publication By default, OpenRG will publish only its main WAN connection, which will be controllable by UPnP entities. However, you may select the 'Publish All WAN Connections' option if you wish to grant UPnP control over all of OpenRG's WAN connections.

6.7.1.2 Granting Remote Access to Your LAN Services Using UPnP

You may also make the services provided by your LAN computers available to computers on the Internet. For example, you may designate a UPnP-enabled Windows PC in your home network to act as a Web server, allowing computers on the Internet to request pages from it. Another example is a game that you may wish to play with other people over the Internet. Some online games require that specific ports be opened to allow communication between your PC and other online players.

- To make your local services available to computers on the Internet:
  1. On your PC (which provides the service), open the 'Network Connections' window.
  2. Right-click 'Internet Connection' and choose 'Properties'. The 'Internet Connection Properties' window appears.

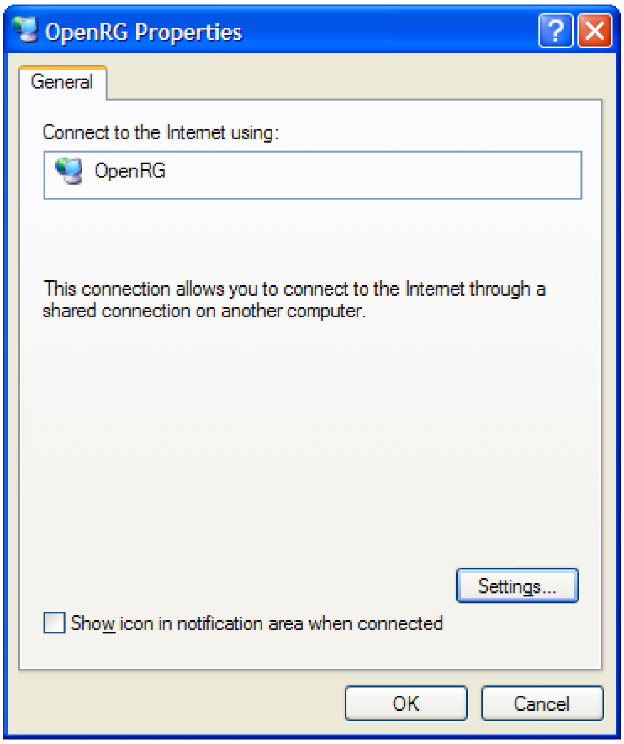


Figure 6.332 Internet Connection Properties

3. Click the 'Settings' button. The 'Advanced Settings' window appears.

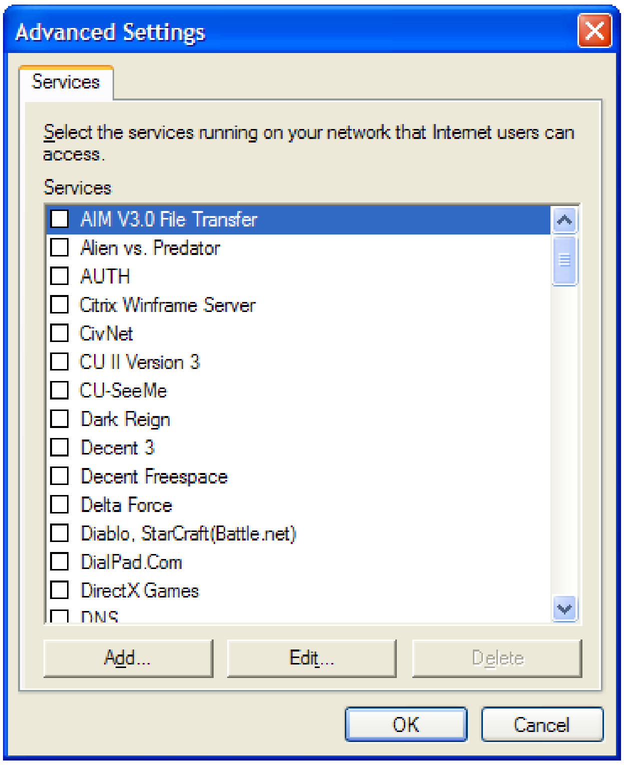


Figure 6.333 Advanced Settings

4. Select a local service that you would like to make available to computers on the Internet. The 'Service Settings' window will automatically appear.

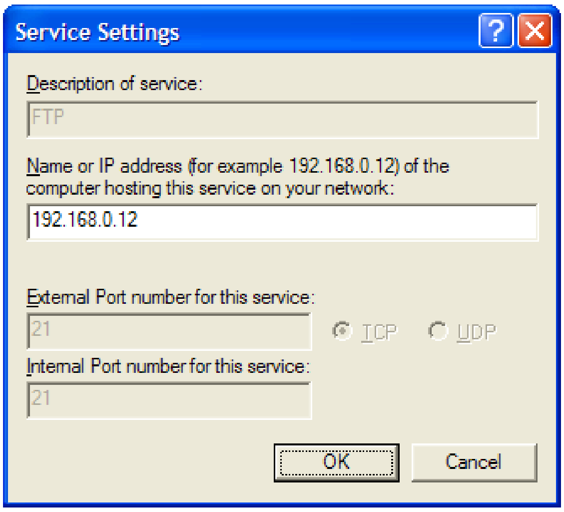


Figure 6.334 Service Settings: Edit Service

5. Enter the PC's local IP address and click 'OK'.

6. Select other services as desired, and repeat the previous step for each.

7. Click 'OK' to save the settings.

- To add a local service that is not listed in the 'Advanced Settings' window:

  1. Follow steps 1-3 above.

  2. Click the 'Add...' button. The 'Service Settings' window appears.

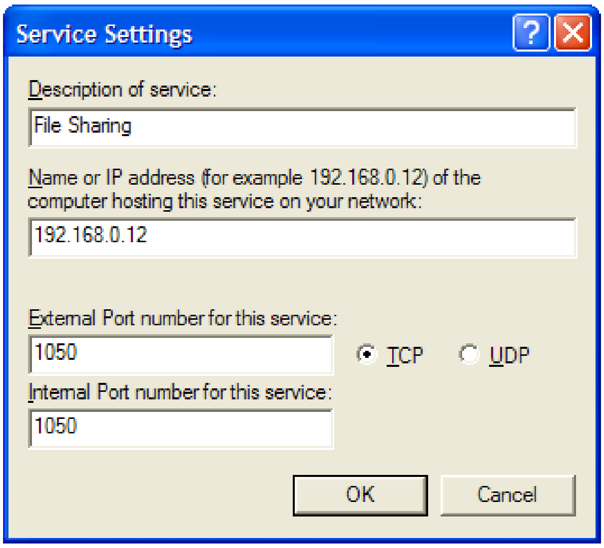


Figure 6.335 Service Settings: Add Service

  3. Complete the fields as indicated in the window.

  4. Click 'OK' to close the window and return to the 'Advanced Settings' window. The service will be selected.

5. Click 'OK' to save the settings.

6.7.2 Simple Network Management Protocol

Simple Network Management Protocol (SNMP) enables network management systems to remotely configure and monitor OpenRG. Your Internet Service Provider (ISP) may use SNMP in order to identify and resolve technical problems. Technical information regarding the properties of OpenRG's SNMP agent should be provided by your ISP. To configure OpenRG's SNMP agent, perform the following:

1. Access this feature either from the 'Management' menu item under the 'System' tab, or by clicking its icon in the 'Advanced' screen. The 'SNMP' screen appears:

Figure 6.336 SNMP Management

2. Specify the SNMP parameters, as provided by your Internet service provider:

Allow Incoming WAN Access to SNMP Select this check box to allow access to OpenRG's SNMP over the Internet.

Read-only/Write Community Names SNMP community strings are passwords used in SNMP messages between the management system and OpenRG. A read-only community allows the manager to monitor OpenRG. A read-write community allows the manager to both monitor and configure OpenRG.

Trusted Peer The IP address, or subnet of addresses, that identify which remote management stations are allowed to perform SNMP operations on OpenRG.

SNMP Traps Messages sent by OpenRG to a remote management station, in order to notify the manager about the occurrence of important events or serious conditions. OpenRG supports both SNMP version 1 and SNMP version 2c traps. Check the Enabled check box to enable this feature. The screen refreshes, displaying the following fields.

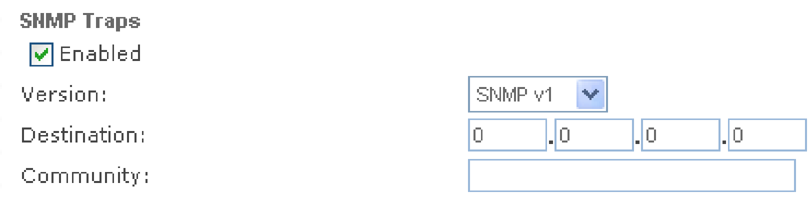


Figure 6.337 SNMP Traps

- **Version** Select between version SNMP v1 and SNMP v2c.
- **Destination** The remote management station's IP address.
- **Community** Enter the community name that will be associated with the trap messages.

6.7.2.1 Defining an SNMPv3 User Account

Simple Network Management Protocol version 3 (SNMPv3) enables you to perform certain management and monitoring operations on OpenRG outside its WBM. Information is exchanged between a management station and OpenRG's SNMP agent in the form of an SNMP message. The advantage of the third version of SNMP over the previous versions is that it provides user authentication, privacy, and access control.

SNMPv3 specifies a User Security Model (USM) that defines the need to create an SNMP user account, in order to secure the information exchange between the management station and the SNMP agent. The following example demonstrates how to define an SNMPv3 user account in OpenRG. Let's assume that you want to add a new SNMPv3 user called "admin". For this purpose, perform the following steps:

1. Add the SNMPv3 user account to the USM table.
2. Associate the user with a new or an existing group.
3. Associate the group with specific views.
4. Create the group views.

Step 1 is performed from OpenRG's CLI. Steps 2–4 are performed from a Linux shell, as in the following example.

1. Add the new user (admin) to the USM table, by running the following `conf set` commands from OpenRG's CLI:

```
OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/name admin

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/security_name admin

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/public ""

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/auth_protocol 1.3.6.1.6.3.10.1.1.1
```

```
OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/priv_protocol 1.3.6.1.6.3.10.1.2.1

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/storage_type 3

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/row_status 1

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/clone_from 0.0

OpenRG> conf set /snmp/mibs/usm_mib/usmuser_table/13.128.0.42.47.128.242.184.29.85.234.15
.79.65.5.97.100.109.105.110/engine_id <ENGINE_ID>
```

The sub-OID 13.128.0.42.47.128.242.184.29.85.234.15.79.65 stands for the engine ID (with length of 13 octets). The decimal values of each engine ID are permanent. The sub-OID 5.97.100.109.105.110 stands for "admin" (5 octets, according to the word length). The decimal values of the user name appear as defined in the ASCII table. The <ENGINE_ID> parameter should be taken from the engine ID in the output of the following command:

```
OpenRG> conf print /snmp/persist_conf
```

Note: You should copy the engine ID without the "0x" prefix.

After the commands specified above are issued, the authentication protocol is set to `usmNoAuthProtocol` (which has OID 1.3.6.1.6.3.10.1.1.1), and the privacy protocol is set to `usmNoPrivProtocol` (which has OID 1.3.6.1.6.3.10.1.2.1).

2. Associate the user with a group. The associated group can be either a new group or an existing group. For example, to add a new group called "admin_group" and associate it with the user "admin", run the following `SNMP SET` commands from a Linux shell:

```
$ snmpset -v2c -c private <OpenRG's IP address> vacmSecurityToGroupStatus.3.5.97.100.109.105
.110 i createAndWait

$ snmpset -v2c -c private <OpenRG's IP address> vacmGroupName.3.5.97.100.109.105.110 s
admin_group

$ snmpset -v2c -c private <OpenRG's IP address> vacmSecurityToGroupStorageType.3.5.97.100
.109.105.110 i nonVolatile

$ snmpset -v2c -c private <OpenRG's IP address> vacmSecurityToGroupStatus.3.5.97.100.109.105
.110 i active
```

The sub-OID 5.97.100.109.105.110 stands for "admin" (with length of 5 octets). These commands populate `vacmSecurityToGroupTable` with a new group called "admin_group".

3. Associate between the group and its views. For example, suppose you want to associate "admin_group" with a view called "admin_view" for reading, writing and notifications, with security level of `noAuthNoPriv`. You can do this by running the following `SNMP SET` commands from a Linux shell:

```
$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessStatus.11.97.100.109.105.110.95
.103.114.111.117.112.0.3.1 i createAndWait

$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessContextMatch.11.97.100.109.105.110
.95.103.114.111.117.112.0.3.1 i exact
```

```
$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessReadViewName.11.97.100.109.105.110
.95.103.114.111.117.112.0.3.1 s admin_view

$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessWriteViewName.11.97.100.109.105
.110.95.103.114.111.117.112.0.3.1 s admin_view

$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessNotifyViewName.11.97.100.109.105
.110.95.103.114.111.117.112.0.3.1 s admin_view

$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessStorageType.11.97.100.109.105.110
.95.103.114.111.117.112.0.3.1 i nonVolatile

$ snmpset -v2c -c private <OpenRG's IP address> vacmAccessStatus.11.97.100.109.105.110.95
.103.114.111.117.112.0.3.1 i active
```

The sub-OID 11.97.100.109.105.110.95.103.114.111.117.112 stands for "admin_group" (with length of 11 octets).

4. Create the needed views. For example, suppose you want to define "admin_view" as a view that includes all the 1.3 subtree. You can do this by running the following `SNMP SET` commands:

```
$ snmpset -v2c -c private <OpenRG's IP address> vacmViewTreeFamilyStatus.10.97.100.109.105
.110.95.118.105.101.119.2.1.3 i createAndWait

$ snmpset -v2c -c private <OpenRG's IP address> vacmViewTreeFamilyType.10.97.100.109.105.110
.95.118.105.101.119.2.1.3 i included

$ snmpset -v2c -c private <OpenRG's IP address> vacmViewTreeFamilyStorageType.10.97.100.109
.105.110.95.118.105.101.119.2.1.3 i nonVolatile

$ snmpset -v2c -c private <OpenRG's IP address> vacmViewTreeFamilyStatus.10.97.100.109.105
.110.95.118.105.101.119.2.1.3 i active
```

The sub-OID 10.97.100.109.105.110.95.118.105.101.119 stands for "admin_view".

After completing these steps, you will have an SNMPv3 user account defined in OpenRG. The following is a sample SNMPv3 query issued to OpenRG's SNMP agent:

```
$ snmpwalk -v 3 -u admin -l noAuthNoPriv 192.168.1.1
```

6.7.3 Enabling Remote Administration

It is possible to access and control OpenRG not only from within the home network, but also from the Internet. This allows you, for example, to view or change your gateway's settings while travelling. It also enables you to allow your ISP to remotely view your gateway's settings and help you troubleshoot functionality and network communication issues.

Remote access to OpenRG is blocked by default to ensure the security of your home network. However, remote access can be provided via the services described further in this section. To view and configure OpenRG's remote administration options, click the 'Remote Administration' link under the 'Management' menu item. Alternatively, click the 'Remote Administration' icon in the 'Advanced' screen. The 'Remote Administration' screen appears.

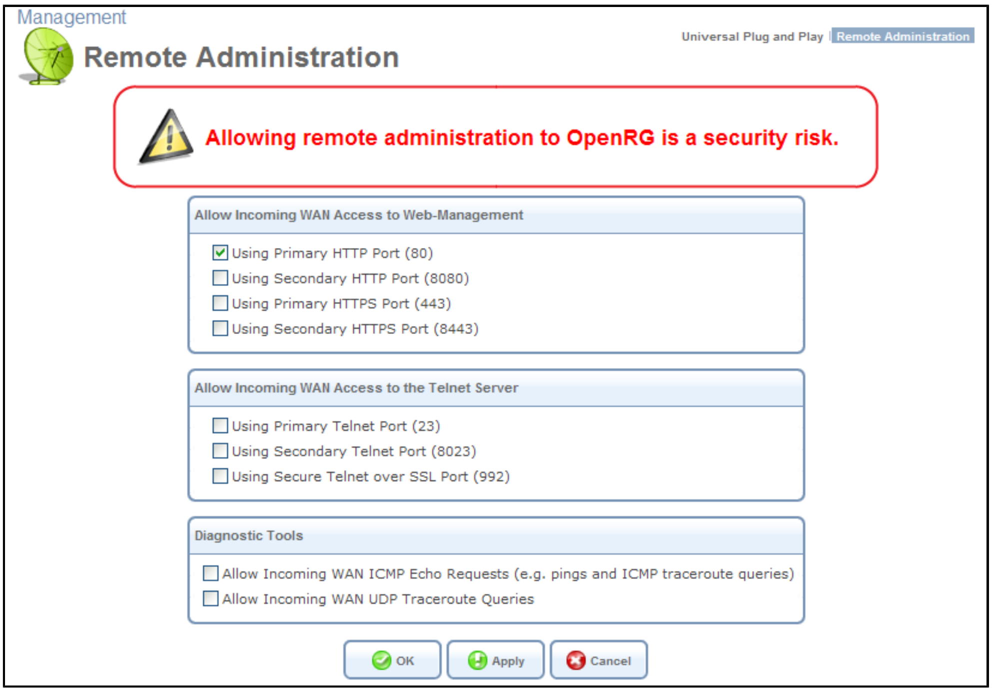


Figure 6.338 Remote Administration

Note that the following management application ports can be configured in the 'System Settings' screen (for more information, refer to Section 6.2).

Allow Incoming Access to Web-Management Used to allow remote access to the WBM via a browser over the selected port(s). Both the secure (HTTPS) and non-secure (HTTP) access can be enabled.

Note that if you select a port other than 80 (which browsers use by default), you will have to specify the port in OpenRG's address when trying to access it. For example, after selecting port 443, you will be able to reach OpenRG's WBM by browsing to:
https://<OpenRG's Internet IP>:443.

Allow Incoming Access to the Telnet Server Used to allow remote access to OpenRG's Telnet server over the selected port(s).

Note: Web Management and Telnet may be used to modify settings of the firewall or disable it. The remote user may also change local IP addresses and other settings, making it difficult or impossible to access the gateway from the home network. Therefore, remote access to Telnet or Web services should only be permitted **when it is absolutely necessary**.

Allow SNMP Control and Diagnostic Requests Used to allow Simple Network Management Protocol (SNMP) requests to remotely configure and monitor OpenRG. For more information, refer to Section 6.7.2.

Diagnostic Tools Used to allow the Ping and Traceroute utilities on a remote computer to communicate with OpenRG in order to test its connectivity.

TR-069 TR-069 is a WAN management protocol intended for communication between Customer Premise Equipment (CPE) and an Auto-Configuration Server (ACS). It defines a

mechanism that encompasses secure auto configuration of a CPE, and also incorporates other CPE management functions into a common framework.

TR-064 As residential gateways offer increasingly complex services, customer premise installation and configuration increase the operators' operational costs. DSL Forum's LAN-Side DSL CPE Configuration protocol, known as TR-064, provides a zero-touch solution for automating the installation and configuration of gateways from the LAN side.

Jungo.net (Jnet) Jungo's proprietary protocol that is used for gateway management from a remote or LAN machine.

- **Enabled** Selecting this check box enables remote management of the gateway via the Jnet protocol.
- **Jungo.net ACS URL** The URL of the Jungo.net Auto-Configuration Server (CONN_MPLEX).
- **Jungo.net Home Page** The URL of the Jungo.net portal.

Additional Jnet Ports This section enables you to set gateway ports for receiving remote management commands over the Jnet and Jnet-SSL protocols.

- **Allow Jnet Commands From Remote Upgrade Server** When this check box is selected, OpenRG allows execution of CLI commands sent from the firmware upgrade server during OpenRG's connection to it (either scheduled or user-initiated). Clicking the 'Remote Upgrade Server URL' link, located under this check box, redirects you to the 'Firmware Upgrade' screen, where you can configure the upgrade settings (for more information, refer to Section 6.8.5).
- **Enable Incoming Jnet Requests to Port 7020** When this check box is selected, OpenRG listens on port 7020 (by default), waiting for CLI commands sent to it from a LAN machine over the Jnet protocol.
- **Allow Incoming WAN Access to Jnet** When this option is selected, OpenRG listens on the WAN port, waiting for CLI commands sent to it from a remote machine over the Jnet protocol.
- **Enable Incoming Jnet-SSL Requests to Port 7021** When this check box is selected, OpenRG listens on port 7021 (by default), waiting for CLI commands sent to it from a LAN machine over the Jnet protocol secured by the SSL.
- **Allow Incoming WAN Access to Jnet** When this option is selected, OpenRG listens on the WAN port, waiting for CLI commands sent to it from a remote machine over the Jnet protocol secured by the SSL.

To allow remote access to OpenRG's administrative services:

1. Select the services that you would like to make available to computers on the Internet. The following should be taken into consideration:

- Although the Telnet service is password-protected, it is not considered a secured protocol. When allowing incoming access to a Telnet server, if port forwarding is configured to use port 23, select port 8023 to avoid conflicts.

- When allowing incoming access to the WBM, if one of your port forwarding rules is configured to use port 80, select port 8080 to avoid conflicts.

> Note: A remote administration service will have precedence over the port forwarding rule created for a local server, when both are configured to utilize the same port. For example, when both the Web server (running on your LAN host) and a remote administration service (utilized by the ISP) are configured to use port 80, OpenRG will grant access to the remote administration traffic. The traffic destined for your Web server will be blocked until you disable the remote administration service or change its dedicated port. For more information about the port forwarding rules created for local servers, refer to Section 5.2.3.

2. Click 'OK' to save the settings.

The encrypted remote administration over the Web, which is performed using a secure (SSL) connection, requires an SSL certificate. When accessing OpenRG for the first time using encrypted remote administration, you will encounter a warning message generated by your browser regarding certificate authentication. This is due to the fact that OpenRG's SSL certificate is self-generated. When encountering this message under these circumstances, ignore it and continue.

It should be noted that even though this message appears, the self-generated certificate is safe, and provides you with a secure SSL connection. It is also possible to assign a user-defined certificate to OpenRG. To learn about certificates, refer to Section 6.9.4.

If you wish to securely administrate OpenRG via its CLI, establish a Telnet over SSL connection to the gateway by performing the following:

1. Select the 'Using Secure Telnet over SSL Port' check box (see Figure 6.338). By default, the secure Telnet over SSL port is 992. You can change the port number in the 'System Settings' screen, as described in Section 6.2.

2. Install a Telnet SSL client on your PC.

3. Connect to OpenRG via Telnet SSL. For example, if you are using a Linux host, enter the following command in a shell:

   ```
   $ telnet-ssl -z ssl 192.168.1.1 992
   ```

   Unless you have a digital certificate recognized by OpenRG, you will be requested to enter OpenRG's username and password.

> Note: If OpenRG's 'Telnet over SSL Client Authentication' option is set to 'Required' (refer to Section 6.2), it is important that the CN field of the certificate contain the

name of the OpenRG user, which has administrator rights. Otherwise, OpenRG will deny access to its CLI.

6.8 Performing System Maintenance

6.8.1 About OpenRG

The 'About OpenRG' screen presents various details about OpenRG's software version, such as version number, type of platform and list of features. In addition, it displays Jungo's contact information.

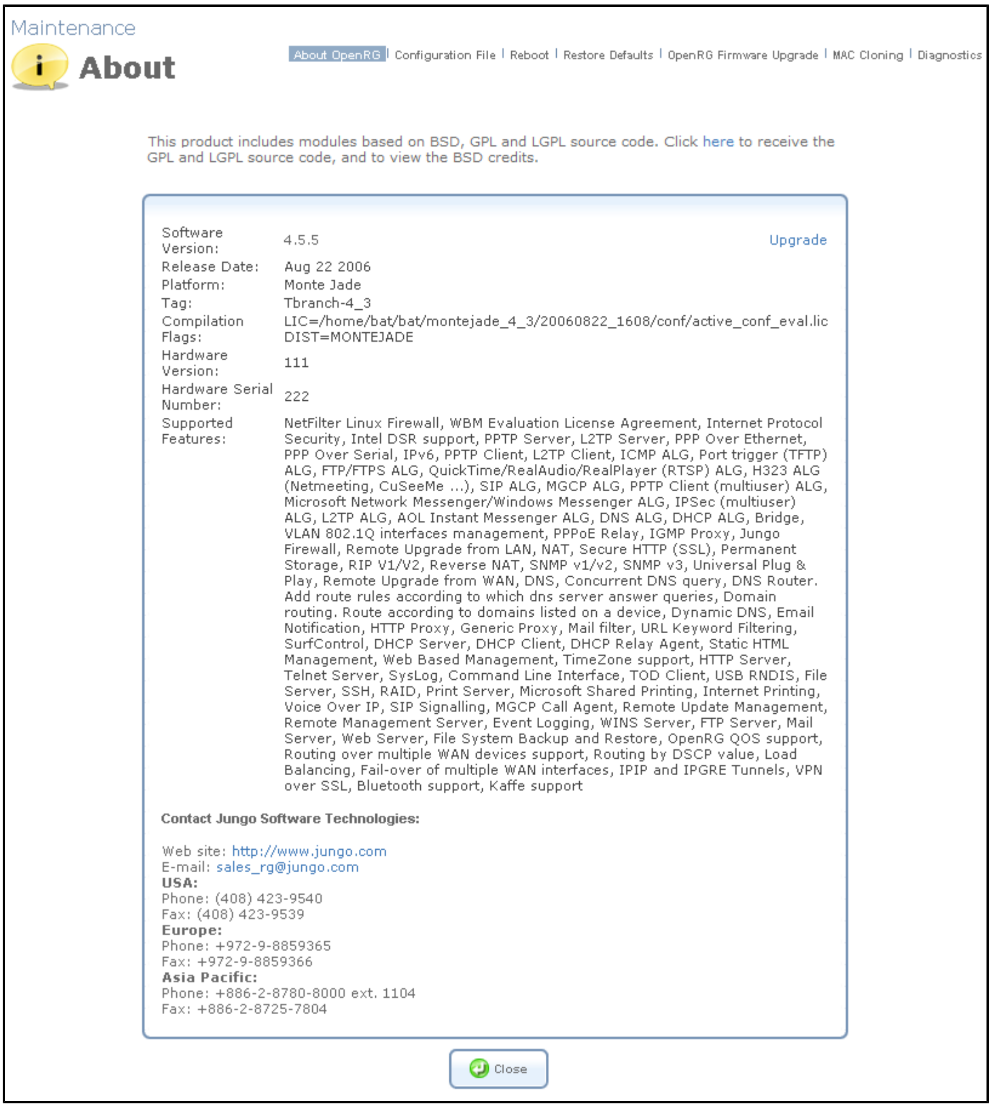


Figure 6.339 About OpenRG

The line at the top of the screen relates to OpenRG's GNU General Public License (GPL) compatibility, and provides a link to the licensing acknowledgement and source code offering page in Jungo's web site. For more information, refer to Chapter 10.

6.8.2 Accessing the Configuration File

OpenRG enables you to view, save and load its configuration file in order to backup and restore your gateway's current configuration. Click the 'Configuration File' link in the links bar to view this file. You can also access it by clicking its icon in the 'Advanced' screen. The 'Configuration File' screen appears, displaying the complete contents of OpenRG's configuration file.

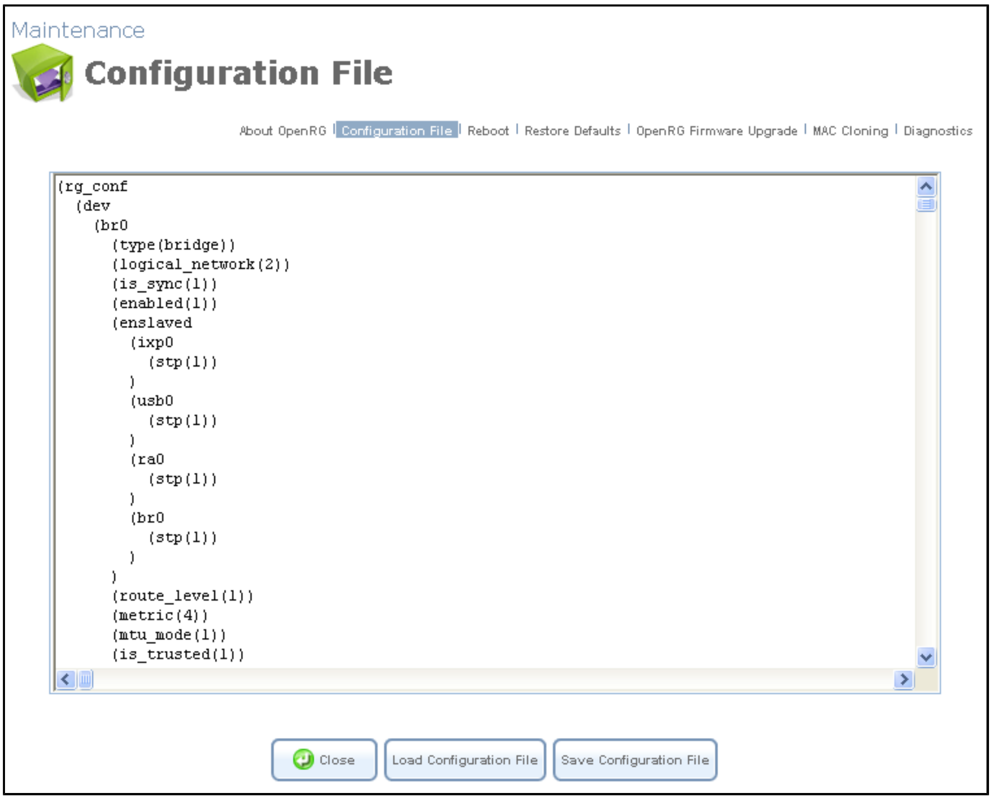


Figure 6.340 Configuration File

Click 'Download Configuration File' to save a copy of your current configuration file on a PC connected to the gateway. Click 'Upload Configuration File' to restore your configuration from a saved file and restart OpenRG.

Note: Upon reboot, OpenRG restores the settings from its configuration file. However, if reboot attempts fail three times consecutively, OpenRG will reset the configuration file by restoring factory defaults before attempting to reboot.

6.8.3 Rebooting Your Gateway

If you wish to reboot your gateway, click the 'Reboot' link under the 'Maintenance' menu item. The 'Reboot' screen appears.

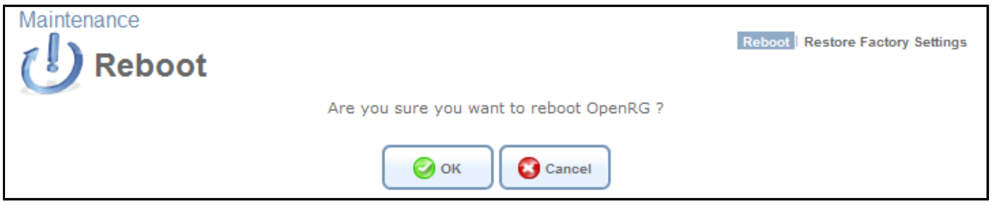


Figure 6.341 Reboot

Click 'OK' to reboot OpenRG. This may take up to one minute. To re-enter the WBM after the gateway is up, click the browser's 'Refresh' button, or browse to OpenRG's local address.

6.8.4 Restoring Factory Settings

Restoring OpenRG's factory settings removes all of the configuration changes made to OpenRG (including the created user accounts). This is useful, for example, when you wish to build your home network from the beginning, and wish to go back to the default configuration.

Click the 'Restore Factory Settings' link under the 'Maintenance' menu item. The 'Restore Factory Settings' appears.

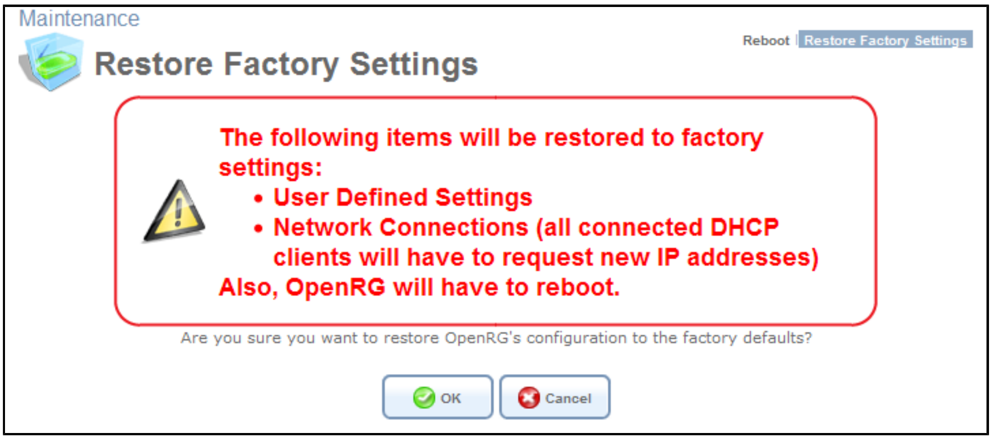


Figure 6.342 Restore Defaults

Click 'OK' to proceed. OpenRG removes all of your personal settings, and then reboots.

6.8.5 Upgrading the Gateway's Firmware

Click the 'OpenRG Firmware Upgrade' link in the links bar. The 'OpenRG Firmware Upgrade' screen appears.

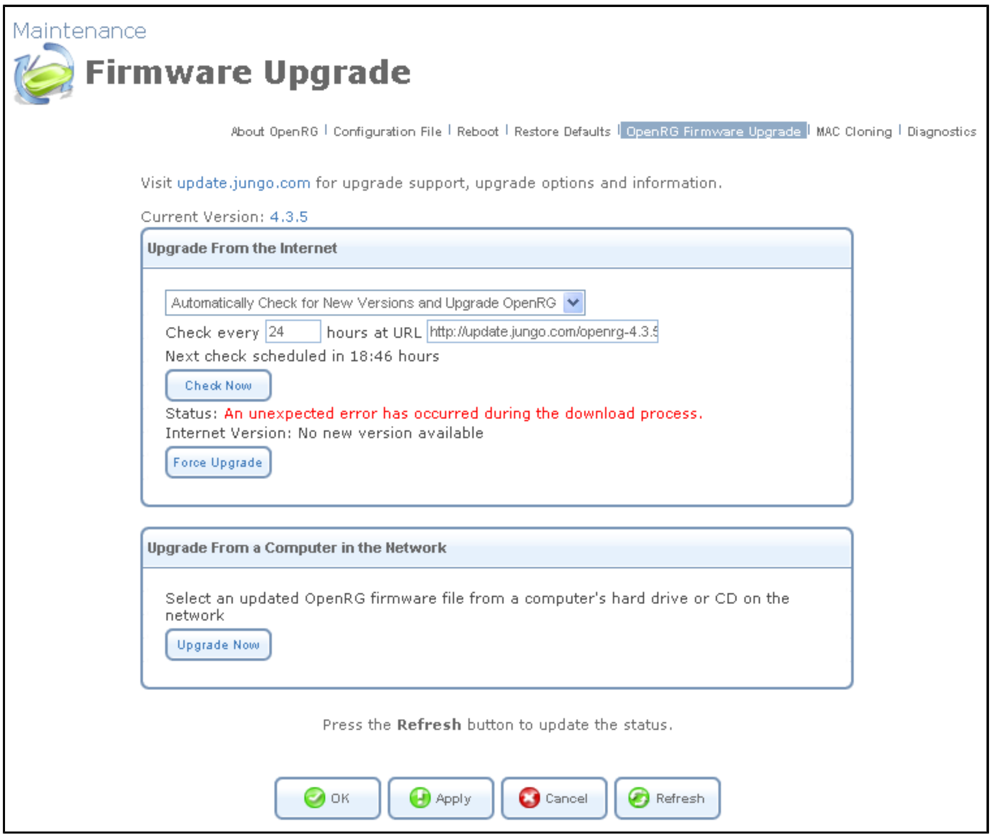


Figure 6.343 OpenRG Firmware Upgrade

OpenRG offers a built-in mechanism for upgrading its software image, without losing any of your custom configurations and settings. There are two methods for upgrading the software image:

- Upgrading from a local computer—use a software image file pre-downloaded to your PC's disk drive or located on the accompanying evaluation CD.
- Upgrading from the Internet—also referred to as *Remote Update*, use this method to upgrade your firmware by remotely downloading an updated software image file.

6.8.5.1 Upgrading From a Local Computer

To upgrade OpenRG's software image using a locally available **.rmt** file, perform the following:

1. In the 'Upgrade From a Computer in the Network' section, click the 'Upgrade Now' button. The 'Upgrade From a Computer in the Network' screen appears.

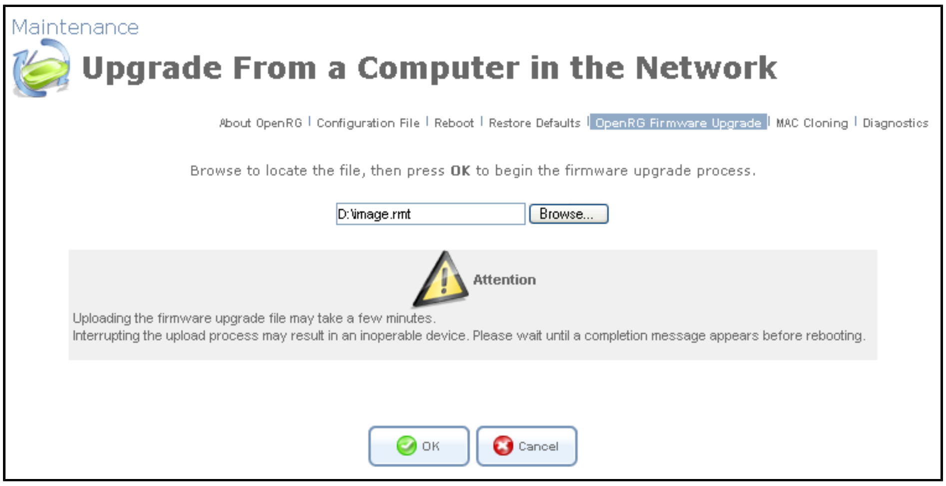


Figure 6.344 Upgrade From a Computer in the Network

2. Enter the path of the software image file, or click the 'Browse' button to browse for the file on your PC, and click 'OK'.

> Note: You can only use files with an ' **rmt** ' extension when performing the firmware upgrade procedure.

The file will start loading from your PC to the gateway. When loading is completed, the following confirmation screen appears, asking if you would like to upgrade to the new version:

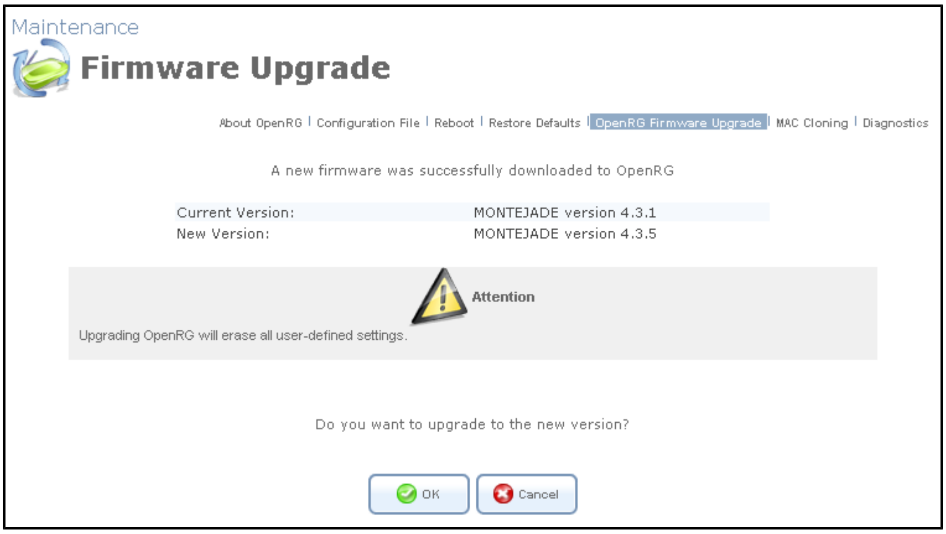


Figure 6.345 Confirm Upgrade

3. Click 'OK' to confirm. When the upgrade process ends, OpenRG automatically reboots, and the login screen of the updated image is displayed. The new software maintains your custom configurations and settings.

6.8.5.2 Upgrading From the Internet

The **Remote Upgrade** mechanism enables you to keep your software image up-to-date, by performing routine daily [1] checks for newer software versions, as well as letting you perform manual checks.

To view the automatic check utility's settings and the last checking result, click the 'OpenRG Firmware Upgrade' icon from the 'Advanced' screen. The 'OpenRG Firmware Upgrade' screen will appear (see Figure 6.343). In the 'Upgrade From the Internet' section, you can select the utility's checking method and interval. The result of the last performed check is displayed between the 'Check Now' and 'Force Upgrade' buttons, indicating whether a new version is available or not.

- If a new version is available:

    1. Click the 'Force Upgrade' button. A download process will begin. When downloading is completed, a confirmation screen will appear (see Figure 6.345), asking whether you wish to upgrade to the new version.

    2. Click 'OK' to confirm. The upgrade process will begin and should take no longer than one minute to complete.

  At the conclusion of the upgrade process, OpenRG will automatically reboot. The new software version will run, maintaining your custom configurations and settings.

- If a new version is unavailable:

    1. Click the 'Check Now' button to perform an immediate check (instead of waiting for the next scheduled one). The screen will display a "Check in progress..." message.

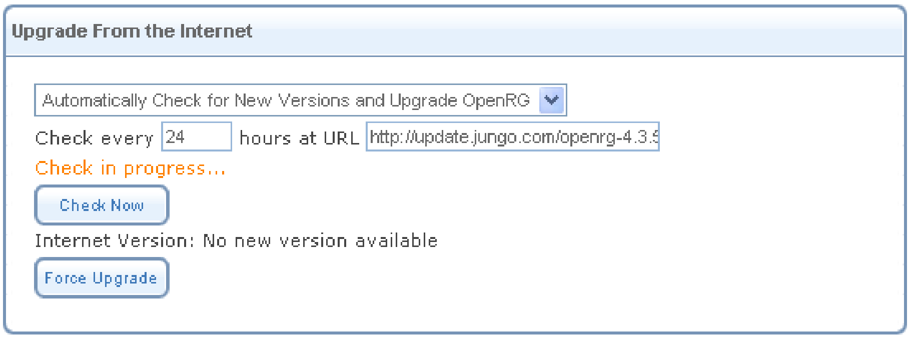


Figure 6.346 Remote Update Check

    2. Click the 'Refresh' button until the check is completed and the result is displayed.

[1] The gateway must be connected to the Internet in order to communicate with the Remote Upgrade server. Systems that store the time internally will attempt to connect and check for an update every 24 hours; systems that lack a BIOS battery will check each time the system restarts and at 24-hour intervals thereafter.

6.8.6 Replacing OpenRG's MAC Address

Click the 'MAC Cloning' link in the links bar. The 'MAC Cloning' screen appears.

Figure 6.347 MAC Cloning Settings

A Media Access Control (MAC) address is the numeric code that identifies a device on a network, such as a modem or a PC network card. After connecting OpenRG, you can replace its MAC address with that of the modem or network card. This is useful, for example, if you are using a static IP address service provided by your ISP. The ISP uses the MAC address to identify the device to which it grants the static IP address. If OpenRG is identified by the replaced MAC address, you can continue receiving the service uninterrupted, and without having to inform your ISP of your newly installed equipment.

To override OpenRG's MAC address with that of the currenly connected modem or network card, click 'Clone My MAC Address'. The MAC address of device connected to OpenRG will replace OpenRG's original one. Click 'OK' to save the changes.

You may also replace OpenRG's MAC address manually, by typing any valid MAC address in the provided fields and clicking 'OK'.

6.8.7 Diagnosing Network Connectivity

Click the 'Diagnostics' link in the links bar. The 'Diagnostics' screen appears.

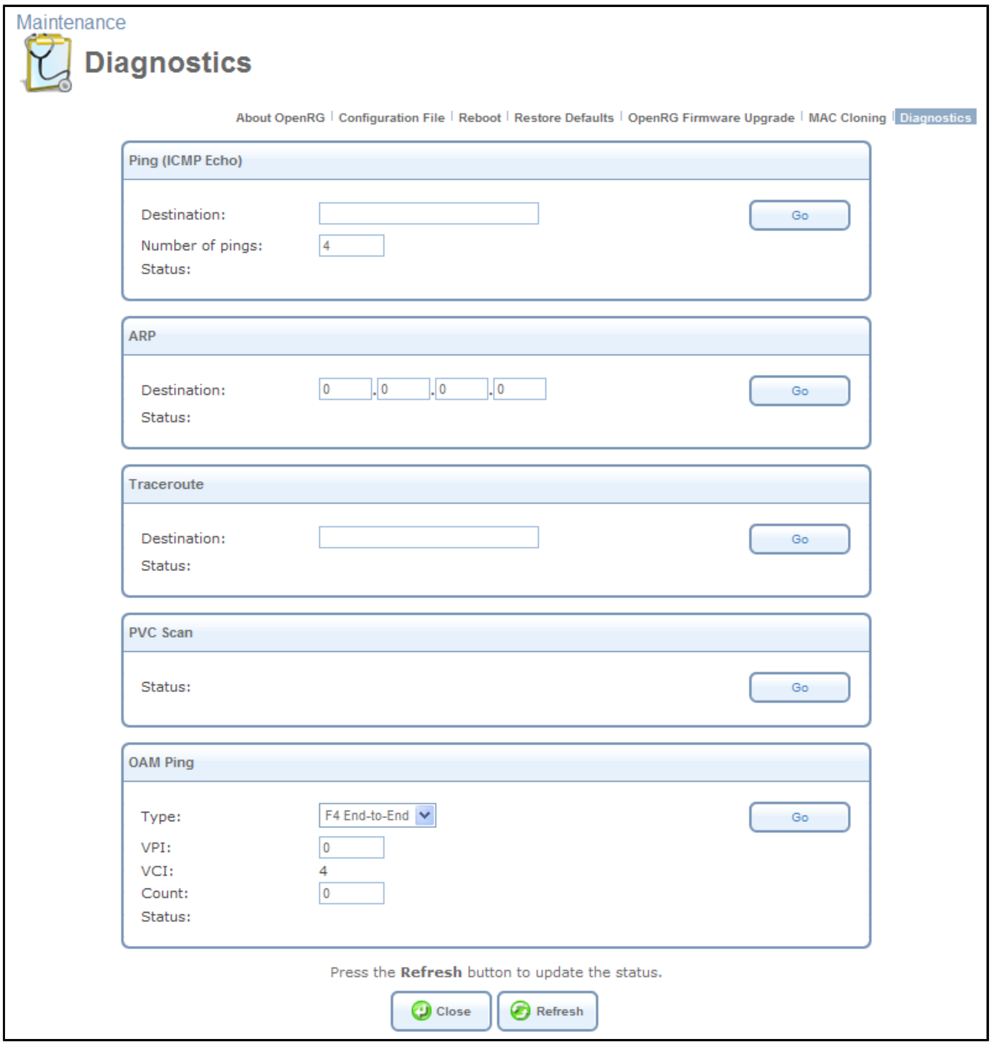


Figure 6.348 Maintenance – Diagnostics

This screen can assist you in testing network connectivity and viewing statistics, such as the number of packets transmitted and received, round-trip time and success status.

Note: The test tools described in this section are platform-dependent, and therefore may not all be available at once.

6.8.7.1 Performing a Ping Test

Use the 'Ping (ICMP Echo)' section to to run a Ping test:

1. In the 'Destination' field, enter the IP address or URL to be tested.
2. Enter the number of pings you would like to run.
3. Click 'Go'.

After a few moments, diagnostic statistics will be displayed. If no new information is displayed, click 'Refresh'.

6.8.7.2 Performing an ARP Test

The Address Resolution Protocol (ARP) test is used to query the physical address (MAC) of a host. Use the 'ARP' section to run an ARP test:

1. In the 'Destination' field, enter the IP address of the target host.
2. Click 'Go'.

After a few moments, diagnostic statistics will be displayed. If no new information is displayed, click 'Refresh'.

6.8.7.3 Performing a Traceroute Test

Use the 'Traceroute' section to run a traceroute test:

1. In the 'Destination' field, enter the IP address or URL to be tested.
2. Click 'Go'. The traceroute test commences, constantly refreshing the screen.
3. To stop the test and view the results, click 'Cancel'.

6.9 Objects and Rules

6.9.1 Viewing and Defining Protocols

The Protocols feature incorporates a list of preset and user-defined applications and common port settings. You can use protocols in various security features such as Access Control and Port Forwarding (refer to Section 5.2.2 and Section 5.2.3 respectively). You may add new protocols to support new applications or edit existing ones according to your needs.

To view the basic protocols list, click the 'Objects and Rules' menu item under the 'System' tab. The 'Protocols' screen appears.

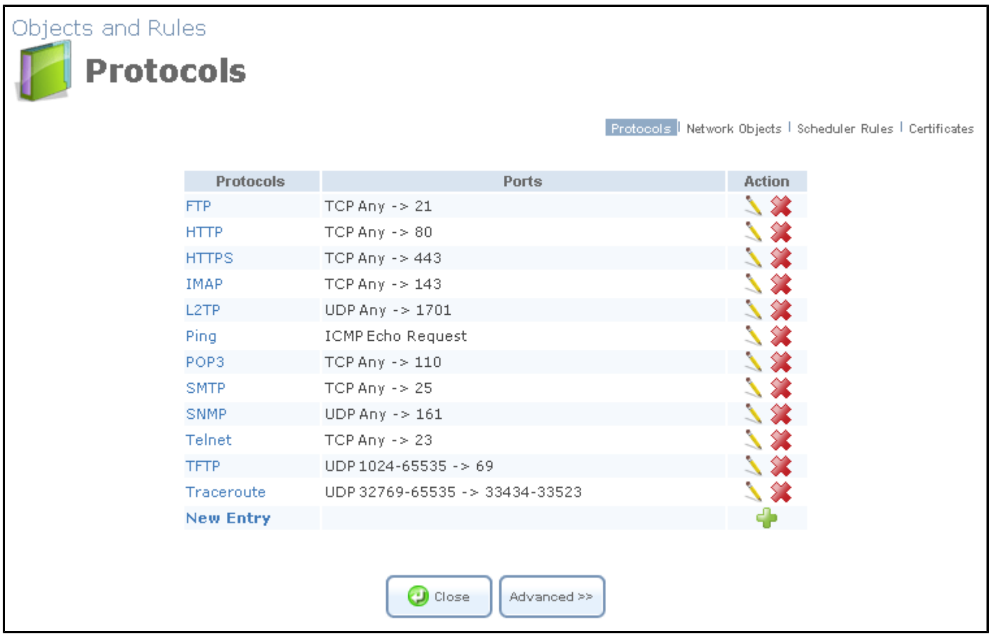


Figure 6.349 Protocols

Click the 'Advanced' button at the bottom of this screen for the full list of protocols supported by OpenRG.

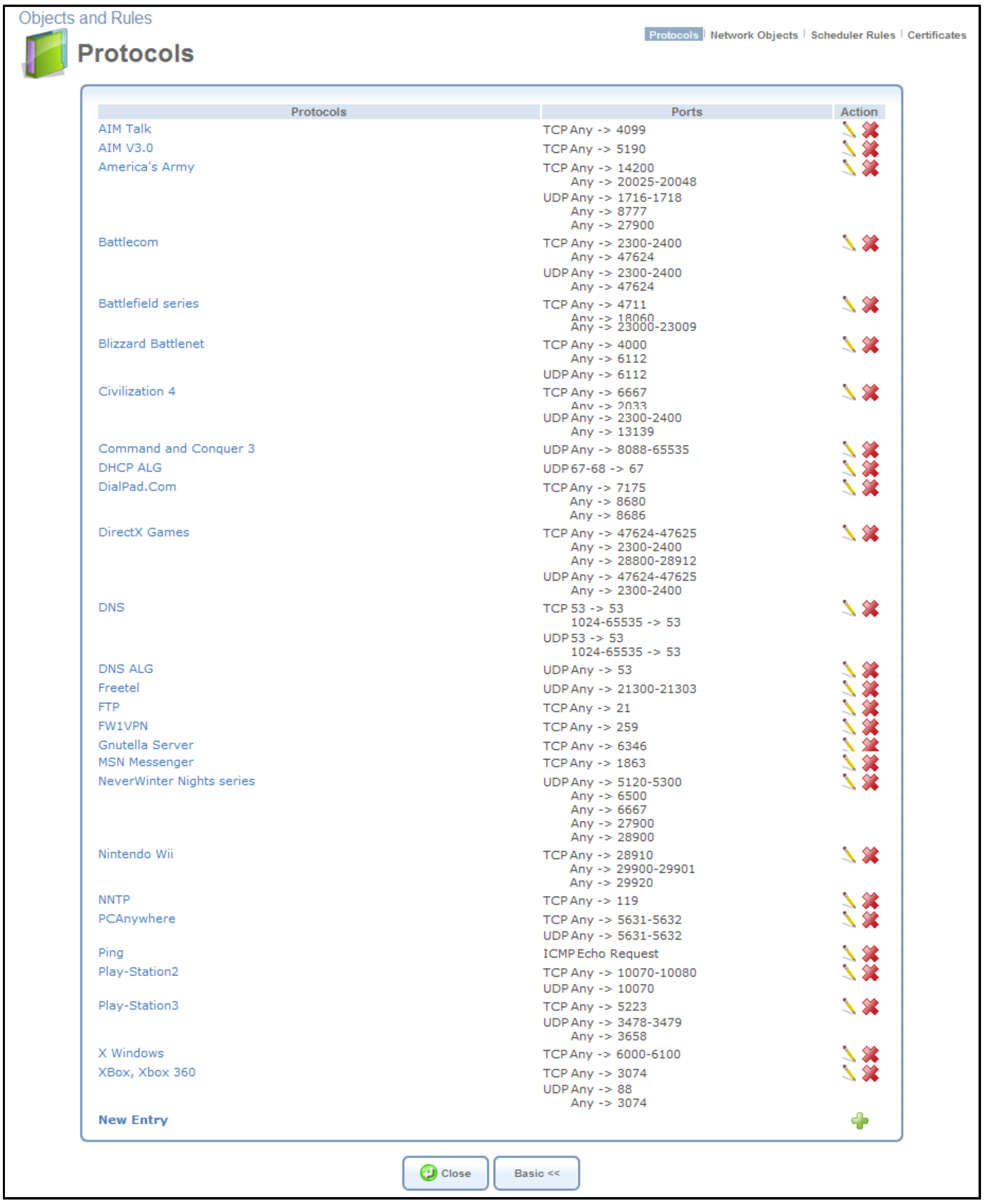


Figure 6.350 Protocols — Advanced Mode

Note that toggling this view between 'Basic' and 'Advanced' is reflected throughout the WBM wherever the protocols list is displayed, and can be set back with 'Show All Services' and 'Show Basic Services', respectively.

To define a protocol:

1. Click the 'New Entry' link in the 'Protocols' screen. The 'Edit Service' screen appears:

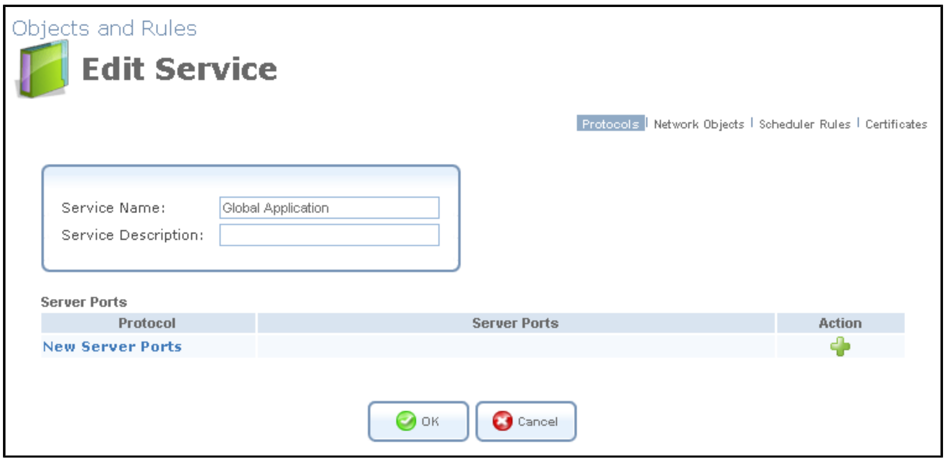


Figure 6.351 Edit Service

2. Name the service in the 'Service Name' field, and click the 'New Server Ports' link. The 'Edit Service Server Ports' screen appears (see Figure 6.352). You may choose any of the protocols available in the drop-down menu, or add a new one by selecting 'Other'. When selecting a protocol from the drop-down menu, the screen refreshes, presenting the respective fields by which to enter the relevant information.

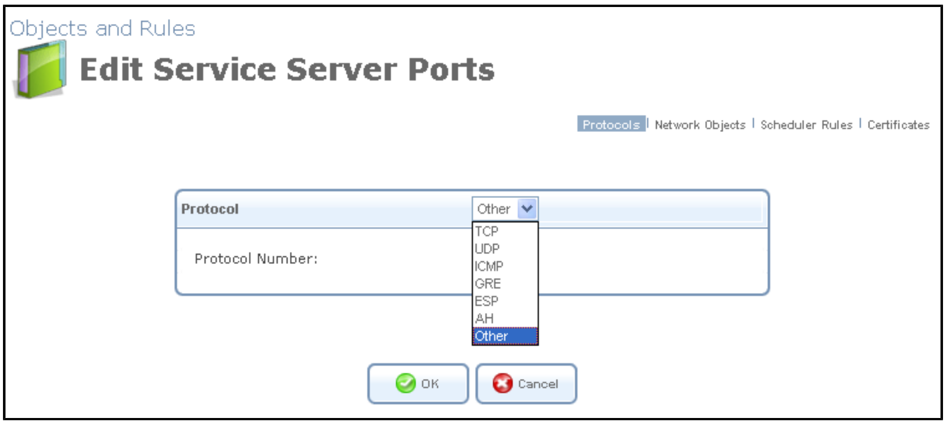


Figure 6.352 Edit Service Server Ports

3. Select a protocol and enter the relevant information.

4. Click 'OK' to save the settings.

6.9.2 Defining Network Objects

Click the 'Network Objects' link in the links bar. The 'Network Objects' screen appears.

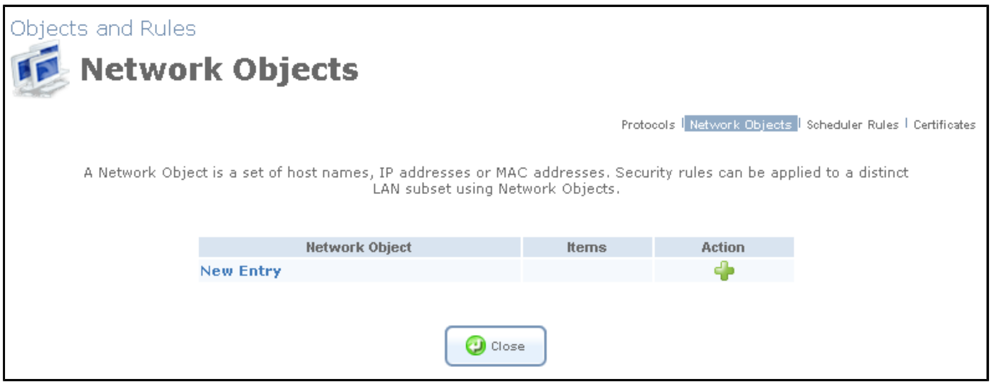


Figure 6.353 Network Objects

Network Objects is a method used to abstractly define a set of LAN hosts, according to specific criteria, such as MAC address, IP address, or host name. Defining such a group can assist when configuring system rules. For example, network objects can be used when configuring OpenRG's security filtering settings such as IP address filtering, host name filtering or MAC address filtering. You can use network objects in order to apply security rules based on host names instead of IP addresses. This may be useful, since IP addresses change from time to time.

It is also possible to define network objects according to MAC addresses, making rule application more persistent against network configuration settings. Moreover, OpenRG supports several DHCP options—60, 61, and 77, enabling the gateway to apply security and QoS rules on a network object according to its unique vendor, client, or user class ID, respectively. For example, a Dell OpenRG™ IP telephone can be identified and applied with specific QoS priority rules.

To define a network object:

1. In the 'Network Objects' screen, click the 'New Entry' link. The 'Edit Network Object' screen appears.

Figure 6.354 Edit Network Object

2. Name the network object in the 'Description' field, and click 'New Entry' to create it. The 'Edit Item' screen appears.

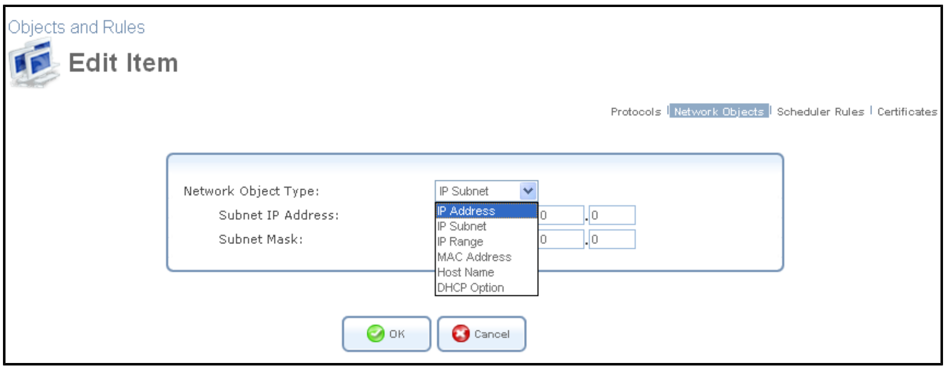


Figure 6.355 Edit Item

When selecting a method from the 'Network Object Type' drop-down menu, the screen refreshes presenting the respective fields for entering the relevant information. The group definition can be according to one of the following methods:

IP Address Enter an IP address common to the group.

IP Subnet Enter a subnet IP address and a subnet mask.

IP Range Enter first and last IP addresses in the range.

MAC Address Enter a MAC address and mask.

Host Name Enter a host name common to the group.

DHCP Option Enter either a vendor class ID (option 60), client ID (option 61), or user class ID (option 77), supplied by your service provider. Note that DHCP clients must also be configured with one of those IDs, in order to be associated with this network object.

3. Select a method and enter the source address accordingly.

4. Click 'OK' to save the settings.

6.9.3 Defining Scheduler Rules

Click the 'Scheduler Rules' link in the links bar. The 'Scheduler Rules' screen appears.

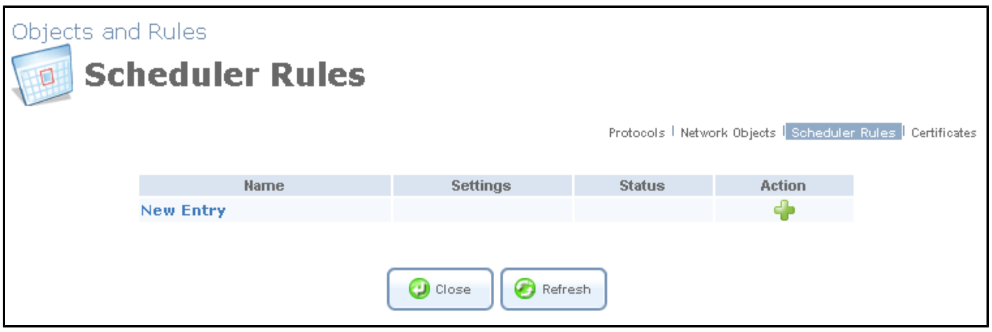


Figure 6.356 Scheduler Rules

Scheduler rules are used for limiting the activation of Firewall rules to specific time periods, specified in days of the week, and hours. To define a rule, perform the following:

1. In the 'Scheduler Rules' screen, click the 'New Entry' link. The 'Edit Scheduler Rule' screen appears.

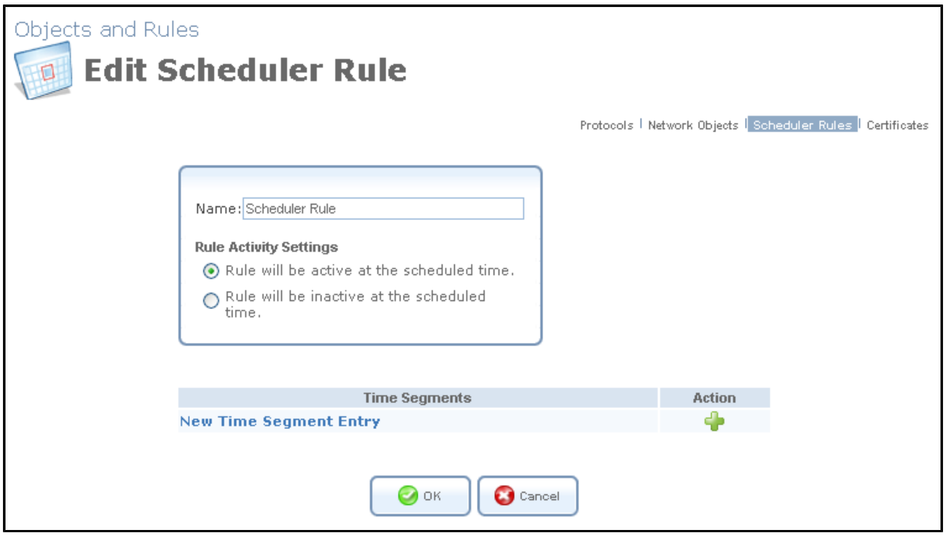


Figure 6.357 Edit Scheduler Rule

2. Specify a name for the rule in the 'Name' field.

3. Click the 'New Time Segment Entry' link to define the time segment to which the rule will apply. The 'Edit Time Segment' screen appears.

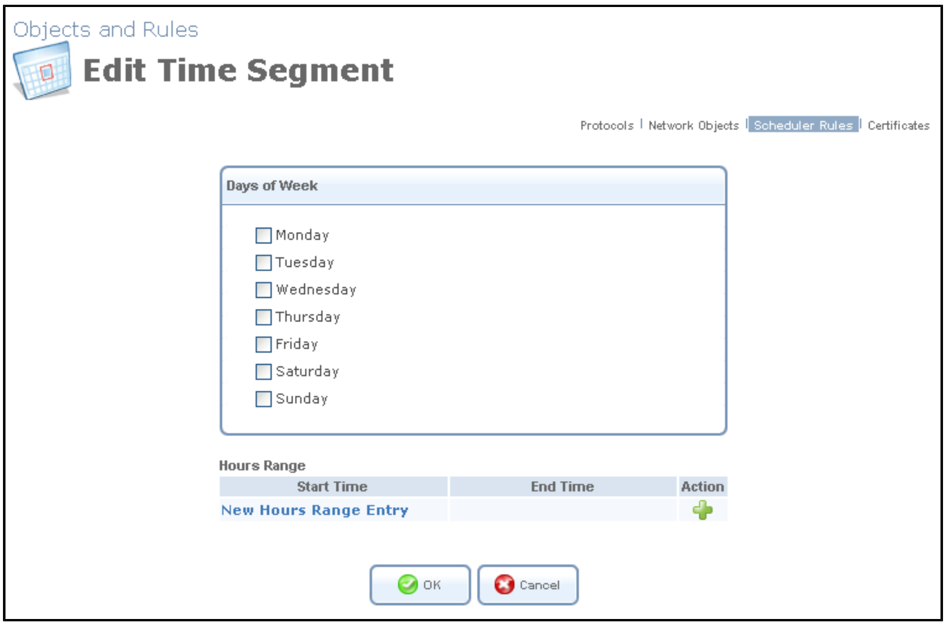


Figure 6.358 Edit Time Segment

   a. Select the day(s) of the week, on which the rule will be activated or deactivated.

b. Click the 'New Hours Range Entry' to narrow the time segment to a specific hour range. The 'Edit Hour Range' screen appears.

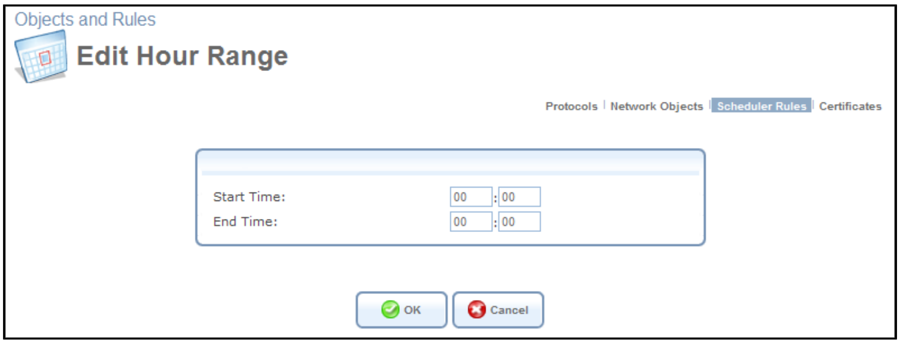


Figure 6.359 Edit Hour Range

c. Enter the desired start and end time values.

> Note: The defined start and end time will be applied to all days of the week you have selected. In addition, if you choose the hour range 21:00-08:00, for example, the rule will be activated on the selected day, and deactivated the next day at 8 o'clock in the morning.

4. Click 'OK' to save the settings. The 'Edit Scheduler Rule' screen appears with the defined time segment.

5. Specify if the rule will be active/inactive during the designated time period, by selecting the appropriate 'Rule Activity Settings' radio button.

6. Click 'OK' to return to the 'Scheduler Rules' screen.

6.9.4 Creating and Loading Digital Certificates

6.9.4.1 Overview

Public-key cryptography uses a pair of keys: a public key and a corresponding private key. These keys can play opposite roles, either encrypting or decrypting data. Your public key is made known to the world, while your private key is kept secret. The public and private keys are mathematically associated; however it is computationally infeasible to deduce the private key from the public key. Anyone who has the public key can encrypt information that can only be decrypted with the matching private key. Similarly, the person with the private key can encrypt information that can only be decrypted with the matching public key.

Technically, both public and private keys are large numbers that work with cryptographic algorithms to produce encrypted material. The primary benefit of public-key cryptography is that it allows people who have no preexisting security arrangement to authenticate each other and exchange messages securely. OpenRG makes use of public-key cryptography to encrypt

and authenticate keys for the encryption of Wireless and VPN data communication, the Web Based Management (WBM) utility, and secured telnet.

6.9.4.1.1 Digital Certificates

When working with public-key cryptography, you should be careful and make sure that you are using the correct person's public key. Man-in-the-middle attacks pose a potential threat, where an ill-intending 3rd party posts a phony key with the name and user ID of an intended recipient. Data transfer that is intercepted by the owner of the counterfeit key can fall in the wrong hands.

Digital certificates provide a means for establishing whether a public key truly belongs to the supposed owner. It is a digital form of credential. It has information on it that identifies you, and an authorized statement to the effect that someone else has confirmed your identity. Digital certificates are used to foil attempts by an ill-intending party to use an unauthorized public key.

A digital certificate consists of the following:

A public key An encryption key that is published and available to anyone.

Certificate information The "identity" of the user, such as name, user ID and so on.

Digital signatures A statement stating that the information enclosed in the certificate has been vouched for by a Certificate Authority (CA).

Binding this information together, a certificate is a public key with identification forms attached, coupled with a stamp of approval by a trusted party.

6.9.4.1.2 X.509 Certificate Format

OpenRG supports X.509 certificates that comply with the ITU-T X.509 international standard. An X.509 certificate is a collection of a standard set of fields containing information about a user or device and their corresponding public key. The X.509 standard defines what information goes into the certificate, and describes how to encode it (the data format). All X.509 certificates have the following data:

The certificate holder's public key the public key of the certificate holder, together with an algorithm identifier that specifies which cryptosystem the key belongs to and any associated key parameters.

The serial number of the certificate the entity (application or person) that created the certificate is responsible for assigning it a unique serial number to distinguish it from other certificates it issues. This information is used in numerous ways; for example when a certificate is revoked, its serial number is placed on a Certificate Revocation List (CRL).

The certificate holder's unique identifier this name is intended to be unique across the Internet. A DN consists of multiple subsections and may look something like this: CN=John Smith, EMAIL=openrg@jungo.com, OU=R&D, O=Jungo, C=US (These refer to the subject's Common Name, Organizational Unit, Organization, and Country.)

The certificate's validity period the certificate's start date/time and expiration date/time; indicates when the certificate will expire.

The unique name of the certificate issuer the unique name of the entity that signed the certificate. This is normally a CA. Using the certificate implies trusting the entity that signed this certificate. (Note that in some cases, such as root or top-level CA certificates, the issuer signs its own certificate.)

The digital signature of the issuer the signature using the private key of the entity that issued the certificate.

The signature algorithm identifier identifies the algorithm used by the CA to sign the certificate.

6.9.4.2 OpenRG Certificate Stores

OpenRG maintains two certificate stores:

1. **OpenRG Local Store** This store contains a list of approved certificates that are used to identify OpenRG to its clients. The list also includes certificate requests that are pending a CA's endorsement. You can obtain certificates for OpenRG using the following methods:

   - Requesting an X509 Certificate – This method creates both a private and a matching public key. The public key is then sent to the CA to be certified.

   - Creating a Self-Signed Certificate – This method is the same as requesting a certificate, only the authentication of the public key does not require a CA. This is mainly intended for use within small organizations.

   - Loading a PKCS#12 Format Certificate – This method loads a certificate using an already available and certified set of private and public keys.

2. **Certificate Authority (CA)** Store This store contains a list of the trusted certificate authorities, which is used to check certificates presented by OpenRG clients.

6.9.4.2.1 Requesting an X509 Certificate

To obtain an X509 certificate, you must ask a CA to issue you one. You provide your public key, proof that you possess the corresponding private key, and some specific information about yourself. You then digitally sign the information and send the whole package (the certificate request) to the CA. The CA then performs some due diligence in verifying that the information you provided is correct and, if so, generates the certificate and returns it. You might think of an X509 certificate as looking like a standard paper certificate with a public key taped to it. It has your name and some information about you on it, plus the signature of the person who issued it to you.

To request an X509 certificate, perform the following:

1. Access this feature either from the 'Objects and Rules' menu item under the 'System' tab, or by clicking its icon in the 'Advanced' screen. The 'OpenRG's Local' sub-tab of the 'Certificates' screen appears.

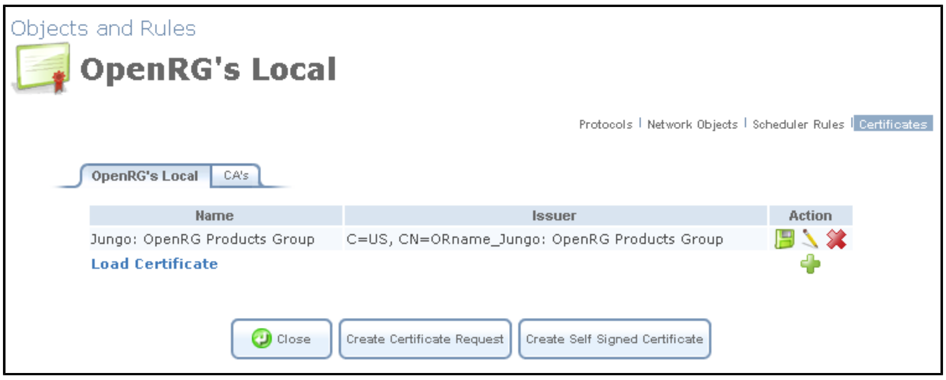


Figure 6.360 Certificate Management

2. Click the 'Create Certificate Request' button. The 'Create X509 Request' screen appears:

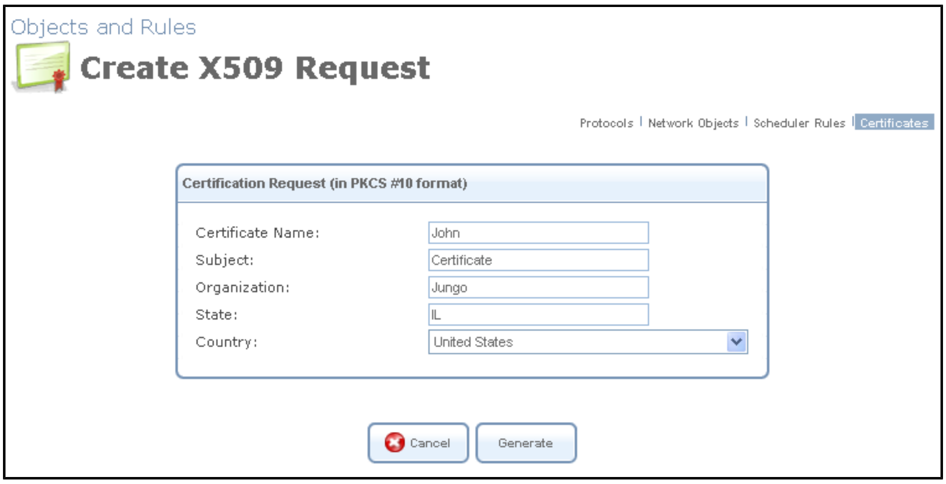


Figure 6.361 Create X509 Request

3. Enter the following certification request parameters:
   - Certificate Name
   - Subject
   - Organization
   - State
   - Country
4. Click the 'Generate' button. A screen appears, stating that the certification request is being generated.

Figure 6.362 Generating a Request

5. After a short while, click the 'Refresh' button, until the 'Download Certificate Request' screen appears.

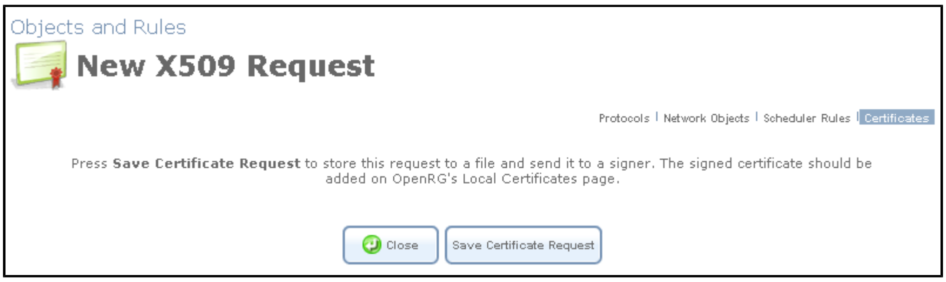


Figure 6.363 Save Certificate Request

6. Click the 'Download Certificate Request' button, and save the request to a file.

7. Click the 'Close' button. The main certificate management screen reappears, listing your certificate as "Unsigned". In this state, the request file may be opened at any time by clicking the  action icon and then 'Open' in the dialogue box (Windows only).

Figure 6.364 Unsigned Certification Request

8. After receiving a reply from the CA in form of a '.pem' file, click the 'Upload Certificate' link. The 'Load OpenRG's Local Certificate' screen appears.

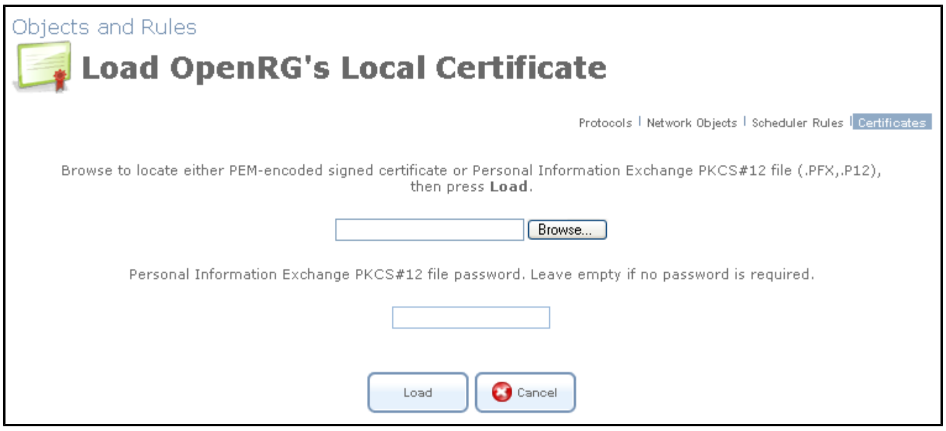


Figure 6.365 Load Certificate

9. Click the 'Browse' button to browse to the signed certificate '.pem' file. Leave the password entry empty and click "Upload" to load the signed certificate. The certificate management screen appears, displaying the certificate name and issuer.

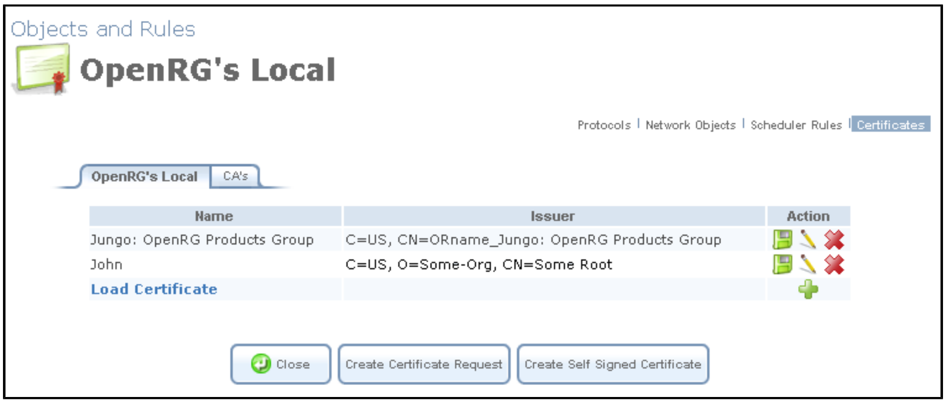


Figure 6.366 Loaded Certificate

10. Click the  action icon and then the 'Open' button in the dialogue box to view the 'Certificate' window (Windows only).

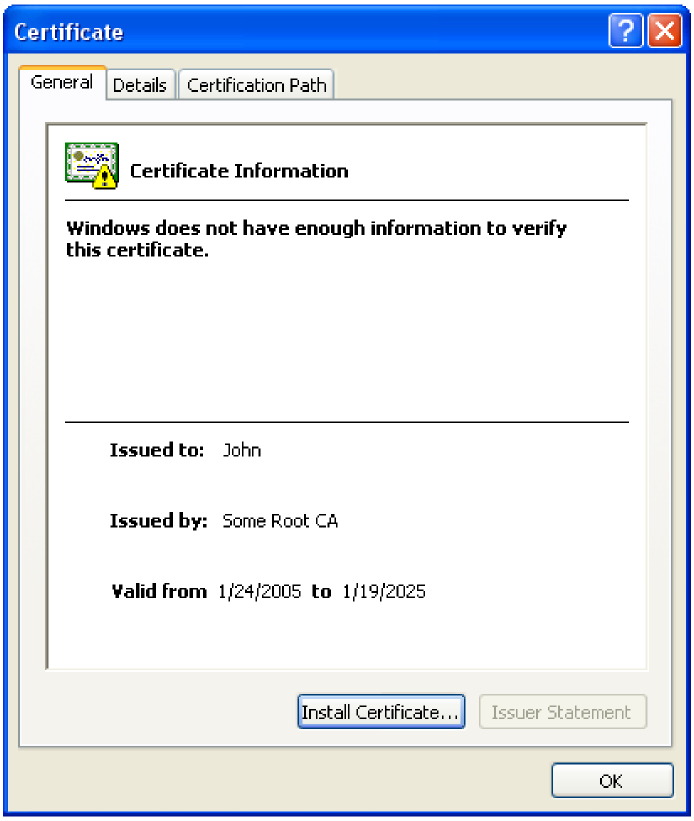


Figure 6.367 Certificate Window

Alternatively, click 'Save' in the dialogue box to save the certificate to a file.

11. You can also click the action icon to view the 'Certificate Details' screen.

Figure 6.368 Certificate Details

6.9.4.2.2 Creating a Self-Signed Certificate

A default self-signed certificate is included in OpenRG, in order to enable certificate demanding services such as HTTPS.

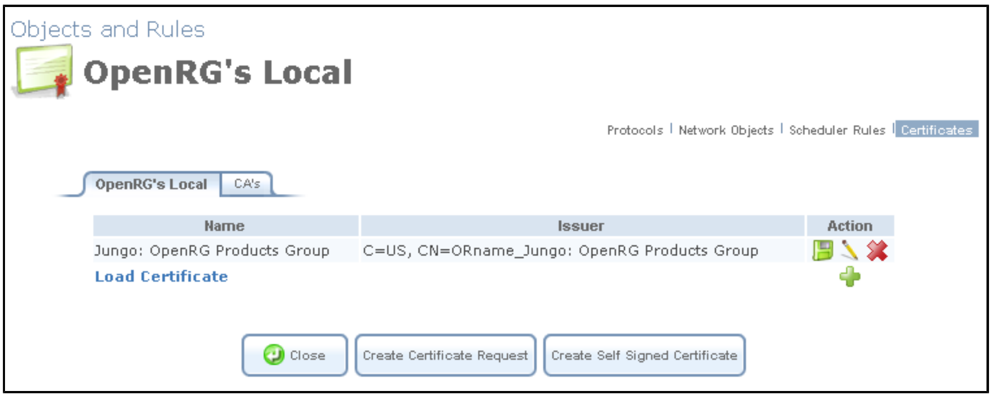


Figure 6.369 Certificates

Note that if deleted, this certificate is restored when OpenRG's Restore Defaults operation is run (refer to Section 6.8.4).

To create a self-signed certificate, perform the following:

1. In the 'OpenRG's Local' sub-tab of the 'Certificates' screen, click the 'Create Self Signed Certificate' button. The 'Create Self Signed X509 Certificate' screen appears.

Figure 6.370 Create Self Signed X509 Certificate

2. Enter the following certification request parameters:
   - Certificate Name
   - Subject
   - Organization
   - State
   - Country
3. Click the 'Generate' button. A screen appears, stating that the certificate is being generated (see Figure 6.371).

Figure 6.371 Generating a Self-Signed X509 Certificate

4. After a short while, click the 'Refresh' button, until the 'Certificate Details' screen appears.

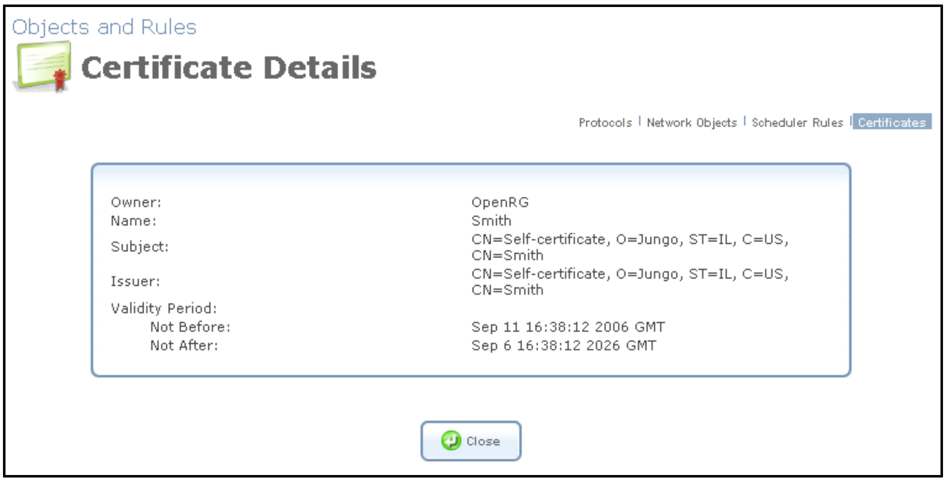


Figure 6.372 Certificate Details

5. Click the 'Close' button. The main certificate management screen reappears, displaying the certificate name and issuer (see Figure 6.373).

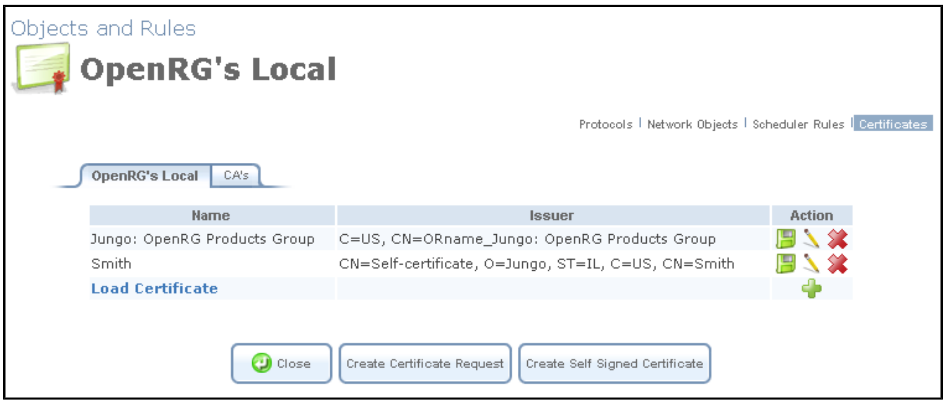


Figure 6.373 Loaded Certificate

6. Click the  action icon and then the 'Open' button in the dialogue box to view the 'Certificate' window (Windows only).

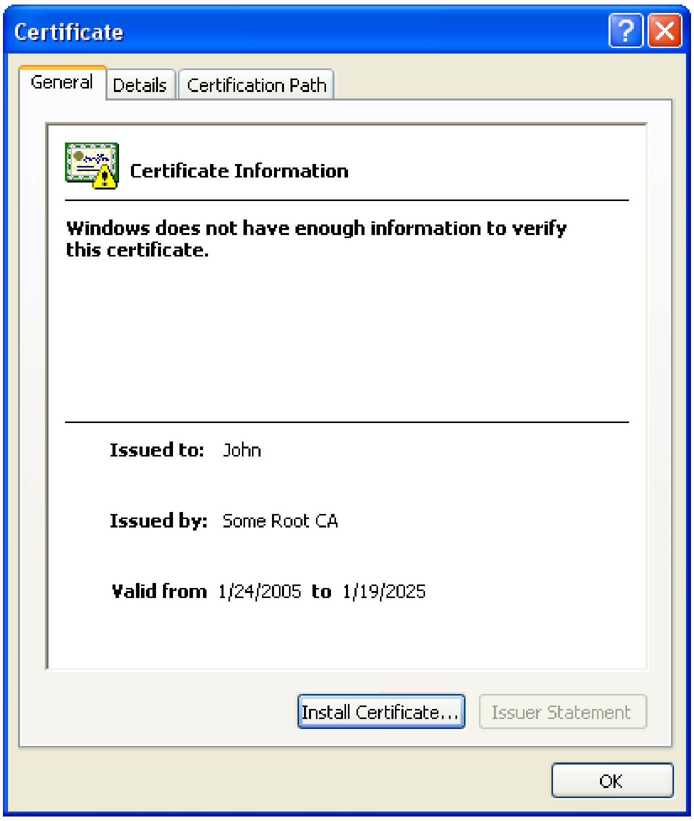


Figure 6.374 Certificate Window

Alternatively, click 'Save' in the dialogue box to save the certificate to a file.

7. You can also click the action icon to view the 'Certificate Details' screen.

Figure 6.375 Certificate Details

6.9.4.2.3 Loading a PKCS#12 Format Certificate

You can load certificates in PKCS#12 format (usually stored in .p12 files) to OpenRG's certificate store. To do so, you must first obtain the '.p12' file, containing the private and public keys and optional CA certificates. Then, perform the following:

1. In the 'OpenRG's Local' sub-tab of the 'Certificates' screen, click the 'Upload Certificate' link. The 'Load OpenRG's Local Certificate' screen appears.

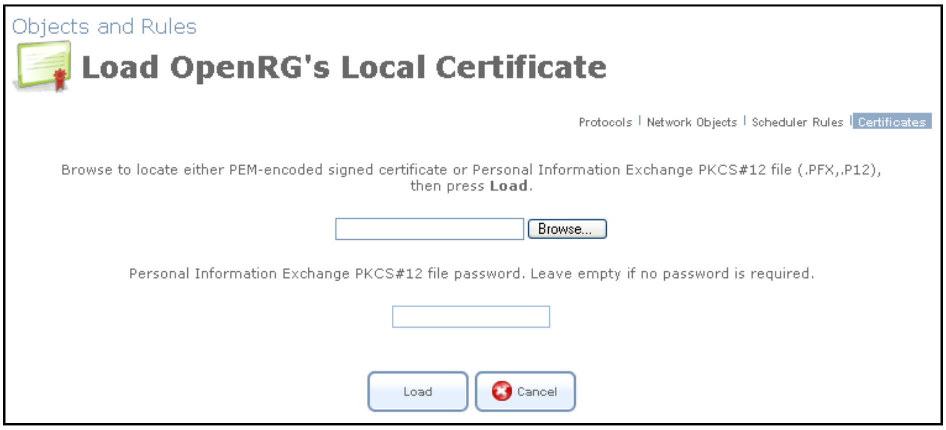


Figure 6.376 Load Certificate

2. Click the 'Browse' button to browse to the '.p12' file. If the private key is encrypted using a password, type it in the password entry (otherwise leave the entry empty), and click "Upload" to load the certificate. The certificate management screen appears, displaying the certificate name and issuer.

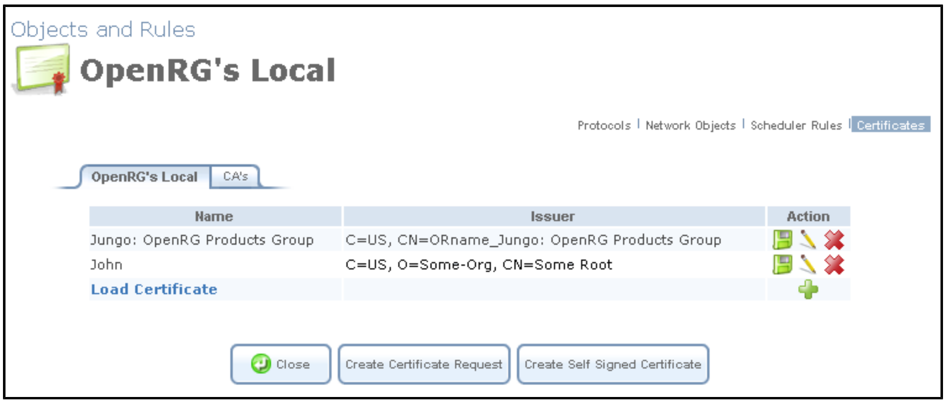


Figure 6.377 Loaded Certificate

If the '.p12' file contained any CA certificates, they will be displayed in the CA store (click the 'CA's' tab to view the CA certificates).

3. Click the action icon and then the 'Open' button in the dialogue box to view the 'Certificate' window (Windows only).

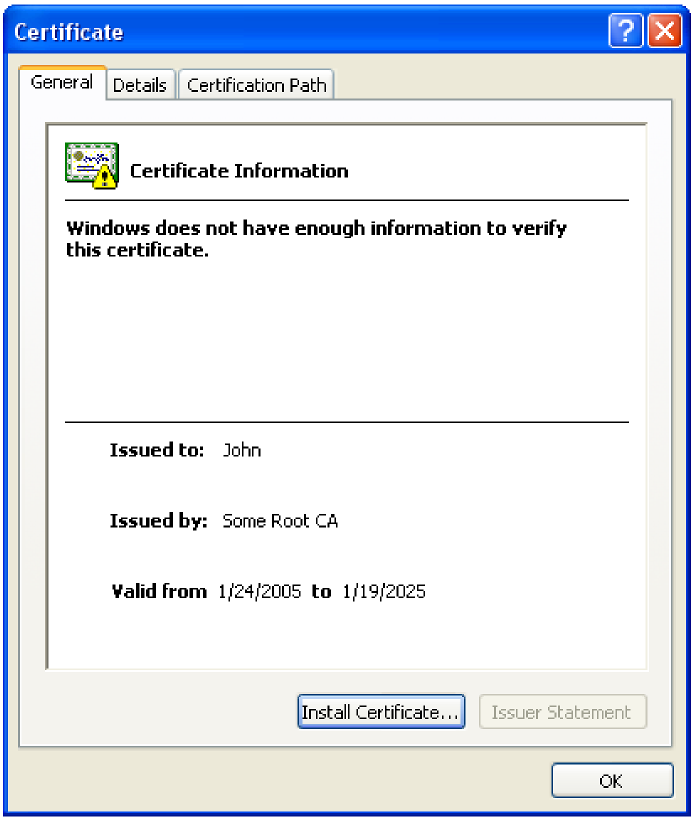


Figure 6.378 Certificate Window

Alternatively, click 'Save' in the dialogue box to save the certificate to a file.

4. You can also click the action icon to view the 'Certificate Details' screen.

Figure 6.379 Certificate Details

6.9.4.2.4 Loading a CA's Certificate

Before you can load a CA's certificate, you must obtain a signed certificate '.pem' or '.p12' file. Then, perform the following:

1. In the 'Certificates' screen, click the 'CA's' sub-tab. The 'CA's' screen appears, displaying a list of certificates.

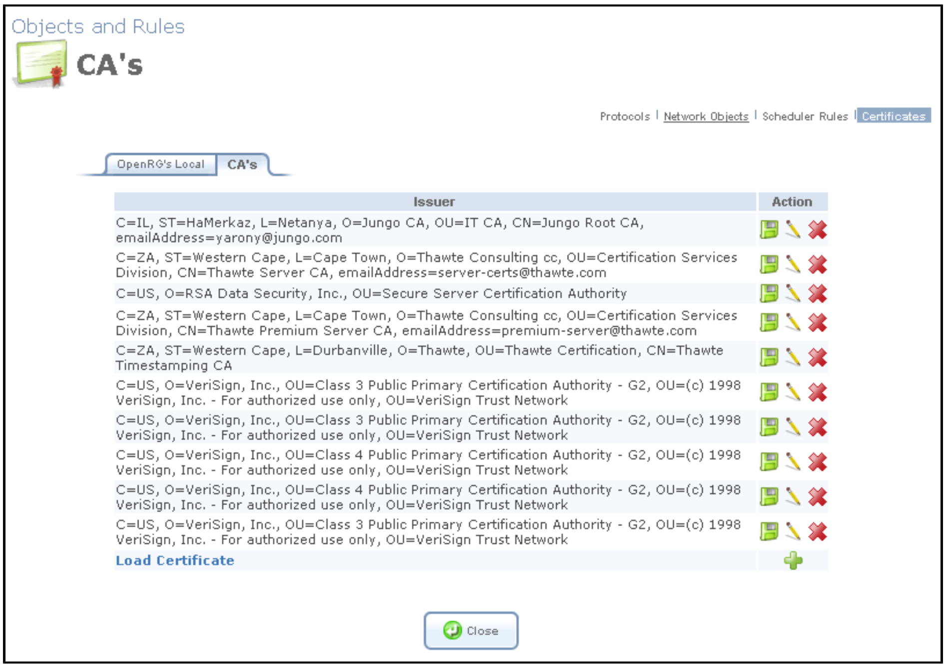


Figure 6.380 CA's Certificates

2. Click the 'Upload Certificate' link. The 'Load CA's Certificate' screen appears.

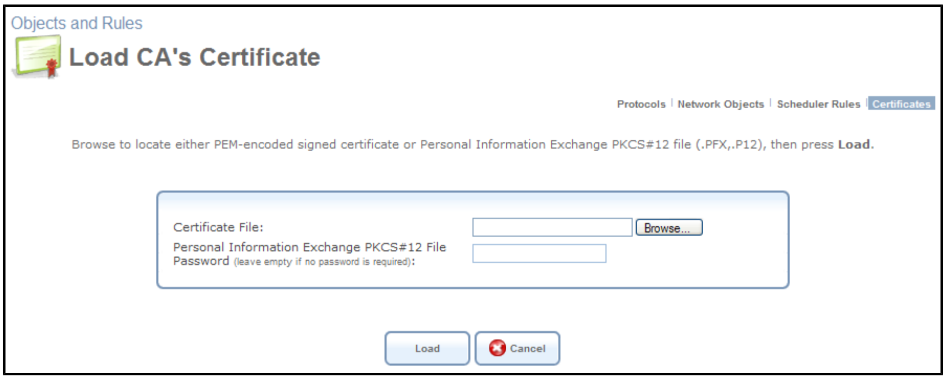


Figure 6.381 Load CA's Certificate

3. Click the 'Browse' button to browse to the '.pem' or '.p12' file. Leave the password entry empty and click "Upload" to load the certificate. The CA Certificates screen reappears (see Figure 6.380), displaying the trusted certificate authority at the bottom of the list.

4. Click the  action icon and then the 'Open' button in the dialogue box to view the 'Certificate' window (Windows only).

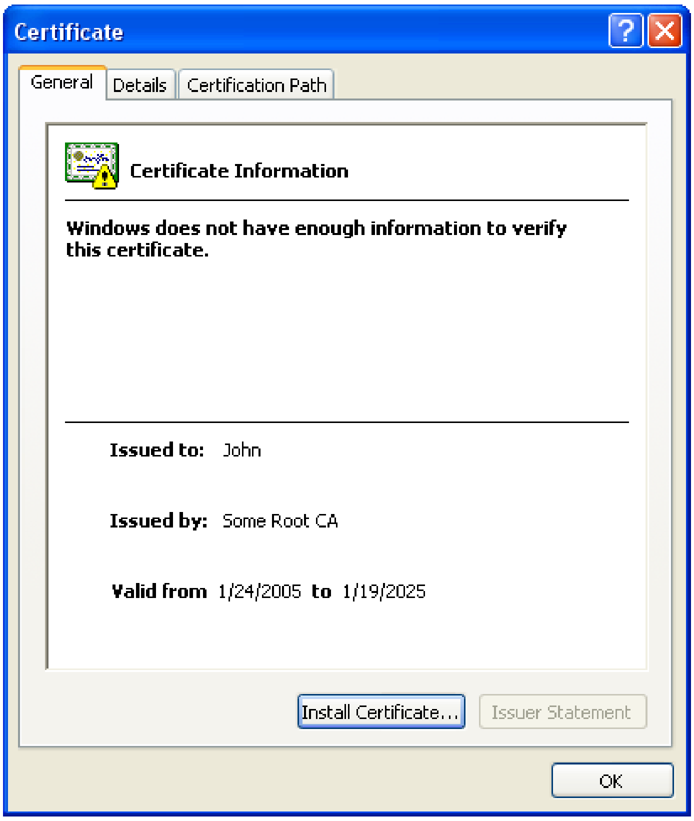


Figure 6.382 Certificate Window

Alternatively, click 'Save' in the dialogue box to save the certificate to a file.

5. You can also click the action icon to view the 'Certificate Details' screen.

Figure 6.383 Certificate Details

Part II Appendix

Table of Contents

7

Configuring a Computer's Network Interface

In most cases, a computer's network interface is configured by default to automatically obtain an IP address. However, a computer with a statically defined IP address and DNS address, for example, may fail to connect to OpenRG. In this case, configure the computer's network interface to obtain its IP and DNS server IP settings automatically. The configuration principle is identical but performed differently on different operating systems. Following are TCP/IP configuration instructions for all supported operating systems.

- **Windows XP**

  1. Access 'Network Connections' from the Control Panel.
  2. Right-click the Ethernet connection icon, and select 'Properties'.
  3. Under the 'General' tab, select the 'Internet Protocol (TCP/IP)' component, and press the 'Properties' button.
  4. The 'Internet Protocol (TCP/IP)' properties window will be displayed.
     a. Select the 'Obtain an IP address automatically' radio button.
     b. Select the 'Obtain DNS server address automatically' radio button.
     c. Click 'OK' to save the settings.

- **Windows 2000/98/Me**

  1. Access 'Network and Dialing Connections' from the Control Panel.

2. Right-click the Ethernet connection icon, and select 'Properties' to display the connection's properties.

3. Select the 'Internet Protocol (TCP/IP)' component, and press the 'Properties' button. The 'Internet Protocol (TCP/IP)' properties will be displayed.

    a. Select the 'Obtain an IP address automatically' radio button.

    b. Select the 'Obtain DNS server address automatically' radio button.

    c. Click 'OK' to save the settings.

- **Linux**

    1. Login into the system as a super-user, by entering "su" at the prompt.

    2. Type "ifconfig" to display the network devices and allocated IP addresses.

    3. Type "pump -i <dev>", where <dev> is the network device name.

    4. Type "ifconfig" again to view the new allocated IP address.

    5. Make sure no firewall is active on device <dev>.

8

List of Acronyms

Acronym	Definition
ALG	Application-Level Gateway
API	Application Programming Interface
CPE	Customer Premise Equipment
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specification
DSL	Digital Subscriber Line
FTP	File Transfer Protocol
HomePNA	Home Phoneline Network Alliance
HTTP	HyperText Transport Protocol
IAD	Integrated Access Device
ICMP	Internet Control Message Protocol
IGMP	Internet Group Multicast Protocol
IP	Internet Protocol
IPSec	IP Security
LAN	Local Area Network
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAPT	Network Address Port Translation
OAM	Operations and Maintenance

OEM	Original Equipment Manufacturer
PDA	Personal Digital Assistant
POP3	Post Office Protocol 3
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
RG	Residential Gateway
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
SPI	Stateful Packet Inspection
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Universal Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network

9

Glossary

PAP Password Authentication Protocol, the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. The Basic Authentication feature built into the HTTP protocol uses PAP.

CHAP Challenge Handshake Authentication Protocol, a type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. The sender and peer must share a predefined secret.

Authentication The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Encryption The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

MPPE Microsoft Point to Point Encryption (MPPE) is a means of representing Point to Point Protocol (PPP) packets in an encrypted form.

Broadcast Broadcasting sends a message to everyone on the network whereas multicasting sends a message to a select list of recipients.

Multicast To transmit a single message to a select group of recipients. A simple example of multicasting is sending an e-mail message to a mailing list. Teleconferencing and videoconferencing also use multicasting, but require more robust protocols and networks.

PPTP Point-to-Point Tunneling Protocol, a technology for creating Virtual Private Networks (VPNs). Because the Internet is essentially an open network, the Point-to-Point Tunneling

Protocol (PPTP) is used to ensure that messages transmitted from one VPN node to another are secure. With PPTP, users can dial in to their corporate network via the Internet.

PPTP IP Security, a set of protocols developed to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs).

VPN A Virtual Private Network (VPN) is a private Network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling Protocol and security procedures.

100Base-T Also known as "Fast Ethernet," an Ethernet cable standard with a data transfer rate of up to 100 Mbps.

10Base-T An older Ethernet cable standard with a data transfer rate of up to 10 Mbps.

802.11, 802.11b A family of IEEE (Institute of Electrical and Electronics Engineers)-defined specifications for wireless networks. Includes the 802.11b standard, which supports high-speed (up to 11 Mbps) wireless data transmission.

802.3 The IEEE (Institute of Electrical and Electronics Engineers - defined specification that describes the characteristics of Ethernet (wired) connections.

Access point A device that exchanges data between computers on a network. An access point typically does not have any Firewall or NAT capabilities.

Ad hoc network A solely wireless computer-to-computer network. Unlike an infrastructure network, an ad hoc network does not include a gateway router.

Adapter Also known as a "network interface card" (NIC). An expansion card or other device used to provide network access to a computer, printer, or other device.

Administrator A person responsible for planning, configuring, and managing the day-to-day operation of a computer network. The duties of an administrator include installing new workstations and other devices, adding and removing individuals from the list of authorized users, archiving files, overseeing password protection and other security measures, monitoring usage of shared resources, and handling malfunctioning equipment.

Bandwidth The amount of information, or size of file, that can be sent through a network connection at one time. A connection with more bandwidth can transfer information more quickly.

Bridge A device that forwards packets of information from one segment of a network to another. A bridge forwards only those packets necessary for communication between the segments.

Broadband connection A high-speed connection, typically 256 Kbps or faster. Broadband services include cable modems and DSL.

Broadband modem A device that enables a broadband connection to access the Internet. The two most common types of broadband modems are cable modems, which rely on cable

television infrastructure, and DSL modems, which rely on telephone lines operating at DSL speeds.

Bus A set of hardware lines used for data transfer among the components of a computer system. A bus essentially allows different parts of the system to share data. For example, a bus connects the disk-drive controller, memory, and input/output ports to the microprocessor.

Cable modem A device that enables a broadband connection to access the Internet. Cable modems rely on cable television infrastructure, in other words, the data travels on the same lines as you cable television.

CAT 5 cable Abbreviation for "Category 5 cable." A type of Ethernet cable that has a maximum data rate of 100 Mbps.

Channel A path or link through which information passes between two devices.

Client Any computer or program that connects to, or requests the services of, another computer or program on a network. For a local area network or the Internet, a client is a computer that uses shared network resources provided by a server.

Client/server network A network of two or more computers that rely on a central server to mediate the connections or provide additional system resources. This dependence on a server differentiating a client/server network from a peer-to-peer network.

Computer name A name that uniquely identifies a computer on the network so that all its shared resources can be accessed by other computers on the network. One computer name cannot be the same as any other computer or domain name on the network.

Crossover cable A type of cable that facilitates network communications. A crossover cable is a cable that is used to interconnect two computers by "crossing over" (reversing) their respective pin contacts.

DHCP Acronym for `Dynamic Host Configuration Protocol'. A TCP/IP protocol that automatically assigns temporary IP addresses to computers on a local area network (LAN). OpenRG supports the use of DHCP. You can use DHCP to share one Internet connection with multiple computers on a network.

Dial-up connection An Internet connection of limited duration that uses a public telephone network rather than a dedicated circuit or some other type of private network.

DMZ Acronym for `demilitarized zone'. A collection of devices and subnets placed between a private network and the Internet to help protect the private network from unauthorized Internet users.

DNS Acronym for `Domain Name System'. A data query service chiefly used on the Internet for translating host names into Internet addresses. The DNS database maps DNS domain names to IP addresses, so that users can locate computers and services through user-friendly names.

Domain In a networked computer environment, a collection of computers that share a common domain database and security policy. A domain is administered as a unit with common rules and procedures, and each domain has a unique name.

Domain name An address of a network connection that identifies the owner of that address in a hierarchical format: server.organization.type. For example, http://www.whitehouse.gov identifies the Web server at the WhiteHouse, which is part of the U.S. government.

Drive An area of storage that is formatted with a file system and has a drive letter. The storage can be a floppy disk (which is often represented by drive A), a hard disk (usually drive C), a CD-ROM (usually drive D), or another type of disk. You can view the contents of a drive by clicking the drive's icon in Windows Explorer or My Computer. Drive C (also known as the hard disk), contains the computer's operating system and the programs that have been installed on the computer. It also has the capacity to store many of the files and folders that you create.

Driver Within a networking context, a device that mediates communication between a computer and a network adapter installed on that computer.

DSL Acronym for `Digital Subscriber Line'. A constant, high-speed digital connection to the Internet that uses standard copper telephone wires.

DSL modem A device that enables a broadband connection to access the Internet. DSL modems rely on telephone lines that operate at DSL speeds.

Duplex A mode of connection. Full-duplex transmission allows for the simultaneous transfer of information between the sender and the receiver. Half-duplex transmission allows for the transfer of information in only one direction at a time.

Dynamic IP address The IP address assigned (using the DHCP protocol) to a device that requires it. A dynamic IP address can also be assigned to a gateway or router by an ISP.

Edge computer The computer on a network that connects the network to the Internet. Other devices on the network connect to this computer. The computer running the most current, reliable operating system is the best choice to designate as the edge computer.

Ethernet A networking standard that uses cables to provide network access. Ethernet is the most widely-installed technology to connect computers together.

Ethernet cable A type of cable that facilitates network communications. An Ethernet cable comes in a couple of flavors. there is twisted pair, and coax Ethernet cables. Each of these allow data to travel at 10Mbit per second.

Firewall A security system that helps protect a network from external threats, such as hacker attacks, originating outside the network. A hardware Firewall is a connection routing device that has specific data checking settings and that helps protect all of the devices connected to it.

Firmware Software information stored in nonvolatile memory on a device.

Flash memory A type of memory that does not lose data when power is removed from it. Flash memory is commonly used as a supplement to or replacement for hard disks in portable computers. In this context, flash memory either is built in to the unit or, more commonly, is available as a PC Card that can be plugged in to a PCMCIA slot.

FTP Acronym for `File Transfer Protocol'. The standard Internet protocol for downloading, or transferring, files from one computer to another.

Gateway A device that acts as a central point for networked devices, receives transmitted messages, and forwards them. OpenRG can link many computers on a single network, and can share an encrypted Internet connection with wired and wireless devices.

Gateway address The IP address you use when you make a connection outside your immediate network.

Hexadecimal A numbering system that uses 16 rather than 10 as the base for representing numbers. It is therefore referred to as a base-16 numbering system. The hexadecimal system uses the digits 0 through 9 and the letters A through F (uppercase or lowercase) to represent the decimal numbers 0 through 15. For example, the hexadecimal letter D represents the decimal number 13. One hexadecimal digit is equivalent to 4 bits, and 1 byte can be expressed by two hexadecimal digits.

HomePNA An industry standard that ensures that through existing telephone lines and a registered jack, computer users on a home network can share resources (such as an Internet connection, files, and printers) without interfering with regular telephone service. HomePNA currently offers data transmission speeds of up to 10 Mbps.

HomeRF An industry standard that combines 802.11b and portable phone standards for home networking. It uses frequency hopping (switching of radio frequencies within a given bandwidth to reduce the risk of unauthorized signal interception). HomeRF offers data transmission speeds of up to 1.6 Mbps at distances of up to 150 feet.

Host name The DNS name of a device on a network, used to simplify the process of locating computers on a network.

Hub A device that has multiple ports and that serves as a central connection point for communication lines from all devices on a network. When data arrives at one port, it is copied to the other ports.

IEEE Acronym for `Institute of Electrical and Electronics Engineers'. A society of engineering and electronics professionals that develops standards for the electrical, electronics, computer engineering, and science-related industries. The IEEE (Eye-triple-E) is a non-profit, technical professional association of more than 377,000 individual members in 150 countries. The full name is the Institute of Electrical and Electronics Engineers, Inc., although the organization is most popularly known and referred to by the letters I-E-E-E.

Infrastructure network A network configuration in which wireless devices connect to a wireless access point (such as OpenRG) instead of connecting to each other directly.

Internet domain In a networked computer environment, a collection of computers that share a common domain database and security policy. A domain is administered as a unit with common rules and procedures, and each domain has a unique name.

Intranet A network within an organization that uses Internet technologies (such a Web browser for viewing information) and protocols (such as TCP/IP), but is available only to certain people, such as employees of a company. Also called a private network. Some intranets offer access to the Internet, but such connections are directed through a Firewall.

IP Acronym for `Internet Protocol'. The protocol within TCP/IP that is used to send data between computers over the Internet. More specifically, this protocol governs the routing of data messages, which are transmitted in smaller components called packets.

IP address Acronym for `Internet Protocol' address. IP is the protocol within TCP/IP that is used to send data between computers over the Internet. An IP address is an assigned number used to identify a computer that is connected to a network through TCP/IP. An IP address consists of four numbers (each of which can be no greater than 255) separated by periods, such as 192.168.1.1.

ISO/OSI reference model Abbreviation for "International Organization for Standardization Open Systems Interconnection" reference model. An architecture that standardizes levels of service and types of interaction for computers that exchange information through a communications network. The ISO/OSI reference model separates computer-to-computer communications into seven protocol layers, or levels; each builds on and relies on the standards contained in the levels below it. The lowest of the seven layers deals solely with hardware links; the highest deals with software interactions at the program level. It is a fundamental blueprint designed to help guide the creation of hardware and software for networks.

ISP Acronym for `Internet service provider'. A company that provides individuals or companies access to the Internet.

Kbps Abbreviation of `kilobits per second'. Data transfer speed, as through a modem or on a network, measured in multiples of 1,000 bits per second.

LAN Acronym for `local area network'. A group of computers and other devices dispersed over a relatively limited area (for example, a building) and connected by a communications link that enables any device to interact with any other on the network.

MAC address Abbreviation for `media access control' address. The address that is used for communication between network adapters on the same subnet. Each network adapter is manufactured with its own unique MAC address.

MAC layer Abbreviation for `media access control' layer. The lower of two sub layers that make up the data-link layer in the ISO/OSI reference model. The MAC layer manages access to the physical network, so a protocol like Ethernet works at this layer.

mapping A process that allows one computer to communicate with a resource located on another computer on the network. For example, if you want to access a folder that resides on another computer, you "map to" that folder, as long as the computer that holds the folder has been configured to share it.

Mbps Abbreviation of `megabits per second'. A unit of bandwidth measurement that defines the speed at which information can be transferred through a network or Ethernet cable. One megabyte is roughly equivalent to eight megabits.

Modem A device that transmits and receives information between computers.

NAT Acronym for `network address translation'. The process of converting between IP addresses used within a private network and Internet IP addresses. NAT enables all of the computers on a network to share one IP address.

Network A collection of two or more computers that are connected to each other through wired or wireless means. These computers can share access to the Internet and the use of files, printers, and other equipment.

Network adapter Also known as a `network interface card' (NIC). An expansion card or other device used to provide network access to a computer, printer, or other device.

Network name The single name of a grouping of computers that are linked together to form a network.

Network printer A printer that is not connected directly to a computer, but is instead connected directly to a network through a wired or wireless connection.

Packet A unit of information transmitted as a whole from one device to another on a network.

PC Card A peripheral device that adds memory, mass storage, modem capability, or other networking services to portable computers.

PCI Acronym for `Peripheral Component Interconnect'. A specific bus type designed to be used with devices that have high bandwidth requirements.

PCI card A card designed to fit into a PCI expansion slot in a personal computer. PCI cards provide additional functionality; for example, two types of PCI cards are video adapters and network interface cards. See PCI.

PCI expansion slot A connection socket designed to accommodate PCI cards.

PCMCIA Acronym for `Personal Computer Memory Card International Association'. A nonprofit organization of manufacturers and vendors formed to promote a common technical standard for PC Card-based peripherals and the slot designed to hold them, primarily on portable computers and intelligent electronic devices.

Peer-to-peer network A network of two or more computers that communicate without using a central server. This lack of reliance on a server differentiates a peer-to-peer network from a client/server network.

PING A protocol for testing whether a particular computer is connected to the Internet by sending a packet to the computer's IP address and waiting for a response.

Plug and Play A set of specifications that allows a computer to automatically detect and configure various peripheral devices, such as monitors, modems, and printers.

Port A physical connection through which data is transferred between a computer and other devices (such as a monitor, modem, or printer), a network, or another computer. Also, a software channel for network communications.

PPPoE Acronym for `Point-to-Point Protocol over Ethernet'. A specification for connecting users on an Ethernet network to the Internet by using a broadband connection (typically through a DSL modem).

Profile A computer-based record that contains an individual network's software settings and identification information.

Protocol A set of rules that computers use to communicate with each other over a network.

Resource Any type of hardware (such as a modem or printer) or software (such as an application, file, or game) that users can share on a network.

Restore factory defaults The term used to describe the process of erasing your base station's current settings to restore factory settings. You accomplish this by pressing the Reset button and holding it for five or more seconds. Note that this is different from resetting the base station.

RJ-11 connector An attachment used to join a telephone line to a device such as a modem or the external telephone lines.

RJ-45 connector An attachment found on the ends of all Ethernet cables that connects Ethernet (wired) cables to other devices and computers

Server A computer that provides shared resources, such as storage space or processing power, to network users.

Shared folder A folder (on a computer) that has been made available for other people to use on a network.

Shared printer A printer (connected to a computer) that has been made available for other people to use on a network.

Sharing To make the resources associated with one computer available to users of other computers on a network.

SNTP Acronym for `Simple Network Time Protocol'. A protocol that enables client computers to synchronize their clocks with a time server over the Internet.

SSID Acronym for `Service Set Identifier', also known as a "wireless network name." An SSID value uniquely identifies your network and is case sensitive.

Static IP address A permanent Internet address of a computer (assigned by an ISP).

Straight-through cable A type of cable that facilitates network communications. An Ethernet cable comes in a couple of flavors. There is twisted pair, and coax Ethernet cables. Each of these allow data to travel at 10Mbit per second. Unlike the Crossover cable, straight-through cable has the same order of pin contacts on each end-plug of the cable.

Subnet A distinct network that forms part of a larger computer network. Subnets are connected through routers and can use a shared network address to connect to the Internet.

Subnet mask Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network

address. Similar in form to an IP address and typically provided by an ISP. An example of a subnet mask value is 255.255.0.0.

Switch A central device that functions similarly to a hub, forwarding packets to specific ports rather than broadcasting every packet to every port. A switch is more efficient when used on a high-volume network.

Switched network A communications network that uses switching to establish a connection between parties.

Switching A communications method that uses temporary rather than permanent connections to establish a link or to route information between two parties. In computer networks, message switching and packet switching allow any two parties to exchange information. Messages are routed (switched) through intermediary stations that together serve to connect the sender and the receiver.

TCP/IP Acronym for `Transmission Control Protocol/Internet Protocol'. A networking protocol that allows computers to communicate across interconnected networks and the Internet. Every computer on the Internet communicates by using TCP/IP.

Throughput The data transfer rate of a network, measured as the number of kilobytes per second transmitted.

USB Acronym for `universal serial bus'. USB (Universal Serial Bus) is a plug-and-play interface between a computer and add-on devices (such as audio players, joysticks, keyboards, telephones, scanners, and printers). With USB, a new device can be added to your computer without having to add an adapter card or even having to turn the computer off.

USB adapter A device that connects to a USB port.

USB connector The plug end of the USB cable that is connected to a USB port. It is about half an inch wide, rectangular and somewhat flat.

USB port A rectangular slot in a computer into which a USB connector is inserted.

UTP Acronym for `unshielded twisted pair'. A cable that contains one or more twisted pairs of wires without additional shielding. It's more flexible and takes less space than a shielded twisted pair (STP) cable, but has less bandwidth.

Virtual server One of multiple Web sites running on the same server, each with a unique domain name and IP address.

WAN Acronym for `wide area network'. A geographically widespread network that might include many linked local area networks.

Wi-Fi A term commonly used to mean the wireless 802.11b standard.

Wireless Refers to technology that connects computers without the use of wires and cables. Wireless devices use radio transmission to connect computers on a network to one another. Radio signals can be transmitted through walls, ceilings, and floors, so you can connect

computers that are in different rooms in the house without physically attaching them to one another.

Wireless access point A device that exchanges data between wireless computers or between wireless computers and wired computers on a network.

Wireless network name The single name of a grouping of computers that are linked together to form a network.

Wireless security A wireless network encryption mechanism that helps to protect data transmitted over wireless networks.

WLAN Acronym for "wireless local area network." A network that exclusively relies on wireless technology for device connections.

10

Licensing Acknowledgement and Source Code Offering

The OpenRG/OpenSMB product may contain code that is subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), and BSD (BSDS) license. The OpenRG/OpenSMB Open Source and GNU Public Licenses page contains:

- With respect to GPL/LGPL: the code package names, license types and locations for the license files, and
- With respect to BSD (BSDS): the code package names with the license texts.

To receive the source code of the GPL/LGPL packages, refer to http://www.jungo.com/openrg/download_gpl.html.

11

Contact Jungo

For additional support, please contact Jungo Software Technologies Ltd.:

Web site:	http://www.jungo.com
E-mail:	Sales: openrg@jungo.com
	Support: rg_support@jungo.com

Jungo Headquarters
3031 Tisch Way
San Jose, CA 95128
U.S.A
Tel. +1 (408) 423 9540
+1 (877) 514 0537
Fax. +1 (877) 514 0538

EMEA
One Heathrow Blvd.
286 Bath Road
West Drayton
Middlesex UB7 0DQ
United Kingdom
Tel. +44 (20) 8476 8481
Fax. +44 (20) 8476 8482

Asia Pacific
P.O.Box 118-757 Taipei
Taipei City 10599
Taiwan (R.O.C)
Tel. +886 (9) 1938 2709

R&D Center
1 Hamachshev Street
Netanya 42504
Israel
Tel. +972 (74) 721 2121
Fax. +972 (74) 721 2122